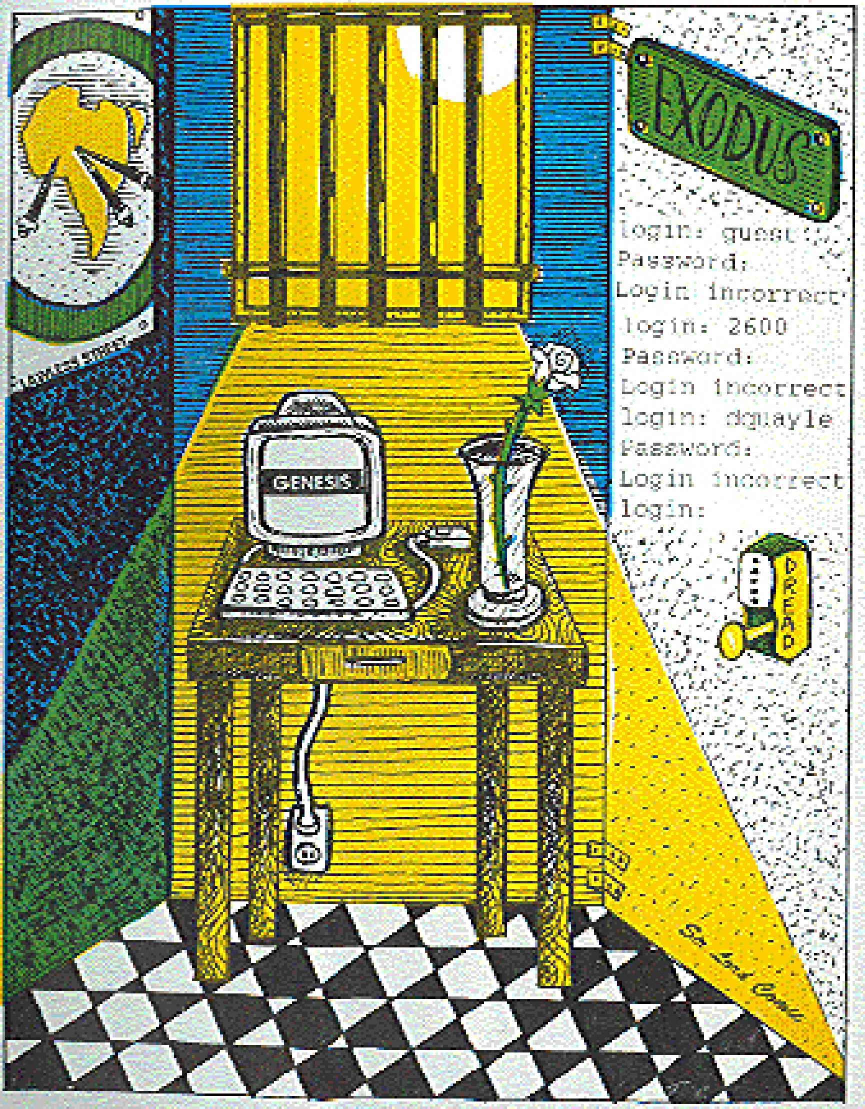
2600

The Hacker Quarterly

VOLUME EIGHT, NUMBER THREE
AUTUMN, 1991

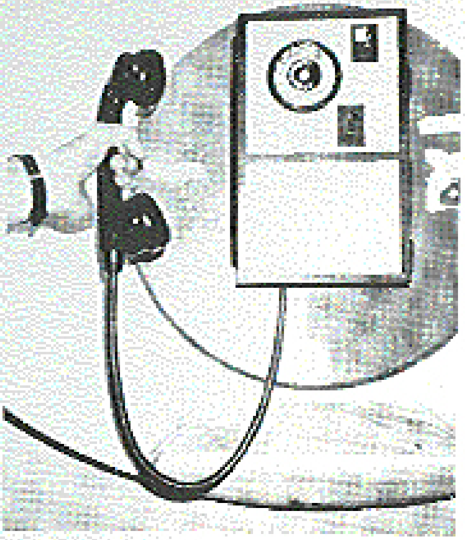


```
login: guest
Password:
Login incorrect
login: 2600
Password:
Login incorrect
login: dquayle
Password:
Login incorrect
login:
```

what it is

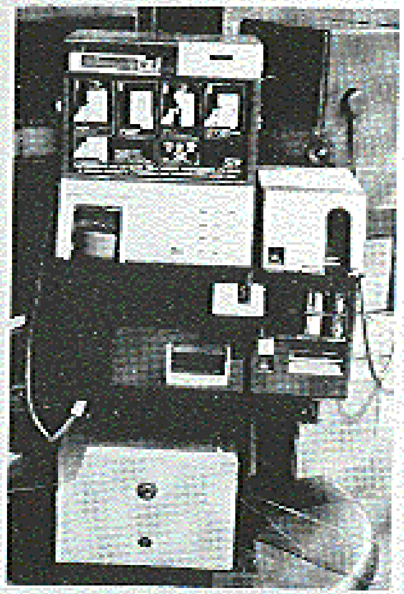
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

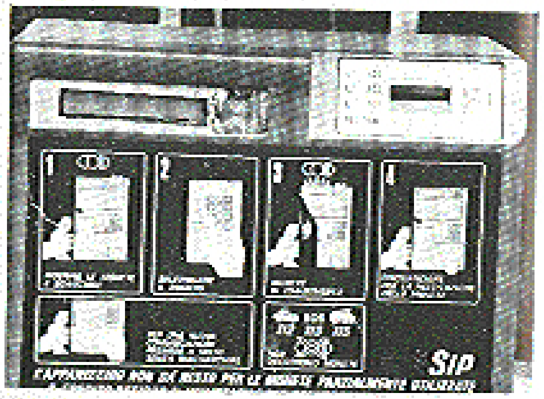
SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851



A Polish Payphone in Warsaw.

Photo by Tom Binko





Orange payphones in Italy. An increasing number only take cards.

Photo by John Drake

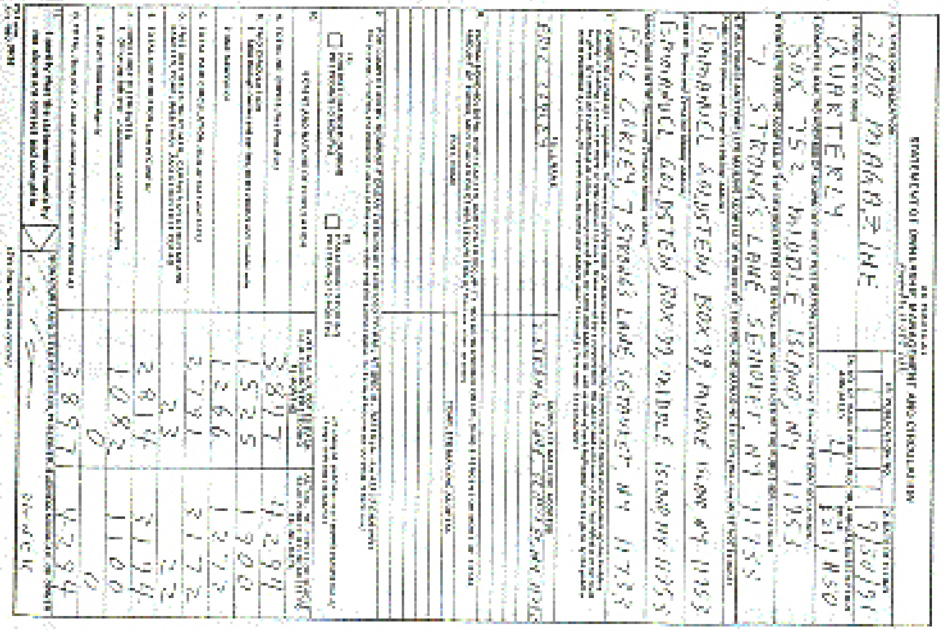
SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. STILL WAITING FOR AFRICAN PAYPHONES.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1991 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**



STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION

2600 MAGAZINE

9/30/91

QUARTERLY

4

$21/$50

BOX 752, MIDDLE ISLAND, NY 11953

7 STRONG'S LANE SETAUKET NY 11733

EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953

EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND NY 11953

ERIC CORLEY, 7 STRONG'S LANE SETAUKET NY 11733

ERIC CORLEY

7 STRONG'S LANE SETAUKET NY 11733

3887	4294
1525	1900
1266	1272
2791	3172
23	22
2814	3194
1073	1100
0	0
3887	4294

Why Won't They Listen?

By this time, we've all witnessed some kind of media report about computer hackers. Whether it's the piece in your newspaper about kids with computers figuring out how to make free phone calls or the special report on television that shows how hackers can gain access to secret corporate computer networks, the angle is almost always the same. And it usually misses the most important points: What kind of data is being stored? Why is it so easy to gain access? And why is there so much gross negligence?

Bearing this in mind, we thought it would be a good idea to bring a couple of stories to the public eye. We felt it was important to share them not only with our readers, but with everyone. And by communicating directly with the press, we could avoid any misconceptions. In fact, the whole thing could be an educational experience.

Our first story concerned easy access to U.S. military computer systems. Over the past few years, Dutch hackers have been able to get into all kinds of systems. This is not because they're necessarily better than American hackers. But they do live in a healthier society where curiosity and exploration are encouraged, not punished. We asked them to show us on videotape just how easy it was to get into a military system. They graciously did this and even we were surprised at how easy it was.

By going to the media and showing them this, we thought that hackers might finally be seen in a better light. After all, with knowledge of military weaknesses, there are plenty of places these hackers could go. But they didn't. They chose to share the information.

Our other story concerned pushbutton locks that are appearing everywhere we look. And while technically this had nothing to do with computers, the similarities were astounding. Here we have a gadget that is supposed to provide security. The average person looks at it and believes what they're told, in much the same way they would believe what a computer tells them without question. But hackers discovered that there was something seriously wrong here. The upshot of our story was that these locks were not locks at all, but open invitations to disaster.

Again, going to the media with this story seemed the proper course of action. Instead of using this knowledge for our own gains, we realized that people had to be warned before it was too late. These locks, which have been used in businesses and offices for years, are now being installed in homes. We knew the media would understand the threat.

What can we say? We were wrong. Despite a massive effort on our part to get every media outlet in the country involved in these stories, the interest we received back was negligible. We held a press conference in New York City, made hundreds of phone calls, did tons of research, and are still paying the bills for it. And it's likely you never heard a single word about it. They decided it just wasn't something the American people needed to hear.

Ironically, in subsequent weeks there were stories in the media of Dutch hackers invading computers yet again. The same old angles. No mention of the efforts of hackers to safeguard these systems. That just wasn't newsworthy.

We think things will change when computer systems with sensitive information are accessed by malevolent people who know what they're doing. They'll change when homes, offices, schools, and mailboxes around the nation are broken into without a trace. We believe that then and only then, the media will take an interest. And, of course, they'll probably decide to blame us. The ratings and circulation will go through the roof.

We did our best to warn the American public of two distinct dangers. It's now up to our readers to spread the word where the media won't.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"They are satisfying their own appetite to know something that is not theirs to know."
- Asst. District Attorney Don Ingraham

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, The Glitch, Bob Hardy, The Infidel, Kevin Mitnick, Knight Lightning, The Plague, David Ruderman, Bernie S., Scott Skinner, Silent Switchman, Mr. Upsetter, Dr. Williams, and those who are elsewhere.

Remote Observations: Geo. C. Tilyou

Shout Outs: Jim Ross, Simplex (for the hours of fun), Len Rose, Franklin, Strong Island Resistance.

SIMPLEX LOCKS

AN ILLUSION OF SECURITY

by Scott Skinner and
Emmanuel Goldstein

No lock is one hundred percent secure. As any locksmith will tell you, even the best lock can be opened if one wishes to invest the time and resources. However, a good lock should at least be secure enough to prevent the average person from compromising it. Common sense dictates that a lock which can easily be opened by anyone is simply not a safe lock to use.

While an average person may not have the necessary skills and expertise to use a lock pick or a blowtorch, almost everyone has the ability to count. And the ability to count is all that is necessary to compromise a Unican/Simplex pushbutton lock. In addition, one needn't count very high. Only 1085 combinations are used, and in most cases this number is reduced considerably.

Anyone can easily open a Simplex lock by merely going through all the possible combinations. As arduous as this may sound, members of *2600* average ten minutes when put to the task. This method becomes even easier if one can find out the "range" of the combination. For instance, if one knows that only three pushbuttons are being used, then one merely has to go through 135 combinations. In this example, a Simplex lock can be compromised in under five minutes. With some models (particularly the commonly used 900 series), a new combination can then be set *without* a key. One can literally lock someone out of their own home.

Far worse than the low number of combinations is the illusion of security that surrounds the lock. We called ten locksmiths at random and were told that "thousands," "millions," and in some cases "a virtually unlimited number" of combinations were available. These claims are somewhat misleading considering the actual number of possible combinations. In addition, no locksmith was able to tell us exactly how many combinations were available, nor did any locksmith believe us when we told them.

Simplex advertisements also claim that these "maximum security" locks are "ideal for security-sensitive areas" and that some models meet the requirements of the Department of Defense Security Manual. We contacted Simplex to find out just what these requirements are. According to Thomas Nazziola, Vice President of Marketing, the locks comply with paragraph *36a* of the Department of Defense Security Manual (DoD 5220.22-M). Mr. Nazziola refused to quote paragraph *36a* of the manual as he felt it was "restricted." However, he summarized the section by claiming that Simplex locks comply with the DoD Security Manual for security-sensitive areas.

2600 was able to obtain a copy of this "restricted" manual just by asking. Upon close examination of paragraph *36a* entitled "Automated Access Control Systems," we were unable to find any information concerning mechanical pushbutton locks. The section that does apply to Simplex locks is paragraph *36b* entitled "Electric, Mechanical, or Electromechanical Devices." According to this section, mechanical devices which meet specified criteria may be used "to control admittance to controlled areas *during working hours*." [emphasis added] While there is an element of truth in Mr. Nazziola's claim, he did not tell us that according to the DoD Security Manual, Simplex locks may not be used as the only

lock source except during "working hours." In addition, it is relatively easy to meet the requirements of the DoD Security Manual. Virtually any combination lock with changeable combinations, and indeed even padlocks, will meet these requirements.

Although Simplex claims that "thousands of combinations are available," in truth only 1085 combinations are used. Another 1085 combinations are available in the guise of "high security half-step codes." These are codes which require the user to push one or more buttons only halfway. Because of the extreme difficulty in setting and using these half-step codes, Simplex advises against their use, and in most cases, does not even inform the user that these codes are available. According to one locksmith, "[Simplex] only suggests it for really high security installations. Government installations. For the average consumer, they don't want anyone to know about it."

We shudder to imagine which high security government installations are using Simplex locks as the only lock source. The "high security codes" are an example of misleading information being used to sell the locks (in this case, to the U.S. government). Naturally, the addition of 1085 combinations does not make the lock considerably more secure. (If 2170 combinations seems like a large number, consider that a $5 Master lock has 64,000.) In addition, we have yet to find one single instance where the half-step codes are used.

We have found that numerous organizations use Simplex locks as the primary lock source. Among the guilty parties in the New York metropolitan area are Federal Express, United Parcel Service (UPS), Citicorp Center, John F. Kennedy International Airport, and the State University of New York at Stony Brook. Others around the nation include General Motors, the State Department, McDonald's, NSA, and the University of Wisconsin.

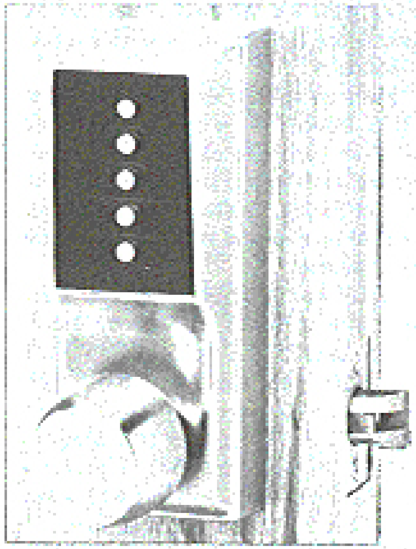
The biggest offender is Federal Express, which uses Simplex locks on over 25,000 dropboxes nationally. According to Robert G. Hamilton, Manager of Corporate Identity [sic] for Federal Express, "[Federal Express dropboxes] are extremely secure. As a matter of fact, there's probably double the cost of security built into these boxes than what's necessary. The idea of having somebody put something extremely important and vital — and it's obviously important and vital or they wouldn't ship it Federal Express — in one of these unmanned receptacles was, I mean security was uppermost on people's minds.... [The dropboxes] are like vaults."

These "vaults" were accessed by members of *2600* in less than ten minutes. The dropboxes are particularly insecure because Federal Express uses the same combination for *all of their dropboxes in every state on the east coast!* So by opening one dropbox, we now have access to thousands.

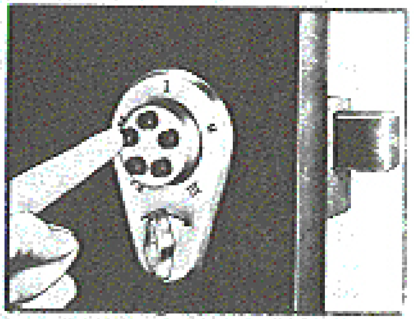
Members of *2600* also gained access to a UPS dropbox — in one shot. UPS did not even bother to change the default combination which is set by Simplex. And just like Federal Express, UPS figures that a single combination is good enough for every dropbox.

Another big offender is the State University of New York at Stony Brook, which uses Simplex locks in both dormitory and academic buildings. According to University Locksmith Gerry Lenox, "I don't consider [the Simplex lock] to be a secure lock. I prefer a deadbolt lock which operates with a key more than I would a Simplex lock.... I think it's more of a convenience lock than it is a security lock." When asked why the university continues to use the lock, Mr.

"The dropboxes are like vaults." - Federal Express

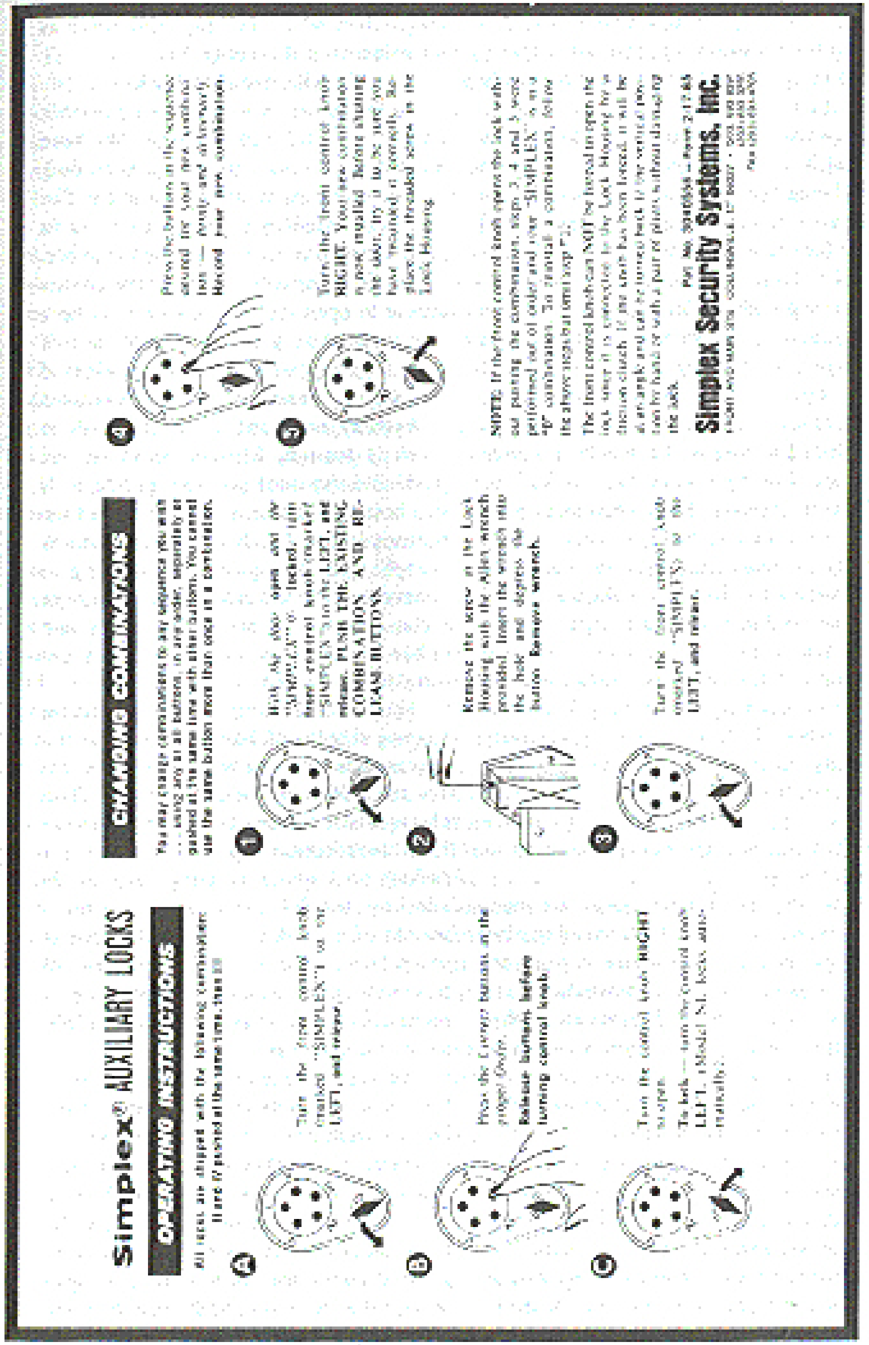


Simplex Series 1000



Simplex Series 900

SIMPLEX LOCKS
TOUCH US ALL
EVERY DAY.
PLEASE TELL US
WHERE YOU FIND
THEM IN YOUR
AREA.



Simplex® AUXILIARY LOCKS

OPERATING INSTRUCTIONS

All locks are shipped with the following combination: II and IV pushed at the same time, then III

A. Turn the front control knob (marked "SIMPLEX") to the LEFT, and release.

B. Press the Correct buttons in the proper Order. **Release buttons before turning control knob.**

C. Turn the control knob **RIGHT** to open.

To lock — turn the control knob LEFT. (Model NL locks automatically).

CHANGING COMBINATIONS

You may change combinations to any sequence you wish ... using any or all buttons, in any order, separately or pushed at the same time with other buttons. You cannot use the same button more than once in a combination.

1. With the door open and the "SIMPLEX"® locked, turn front control knob (marked "SIMPLEX") to the LEFT, and release. PUSH THE EXISTING COMBINATION AND RELEASE BUTTONS.

2. Remove the screw in the Lock Housing with the Allen wrench provided. Insert the wrench into the hole and depress the button. **Remove wrench.**

3. Turn the front control knob (marked "SIMPLEX") to the LEFT, and release.

4. Press the buttons in the sequence desired for your new combination — firmly and deliberately. Record your new combination.

5. Turn the front control knob RIGHT. Your new combination is now installed. Before shutting the door, try it to be sure you have recorded it correctly. Replace the threaded screw in the Lock Housing.

NOTE: If the front control knob opens the lock without pushing the combination, steps 3, 4 and 5 were performed out of order and your "SIMPLEX" is at a "0" combination. To reinstall a combination, follow the above steps but omit step "2".

The front control knob can NOT be forced to open the lock since it is connected to the Lock Housing by a friction clutch. If the knob has been forced, it will be at an angle and can be turned back to the vertical position by hand or with a pair of pliers without damaging the lock.

Pat. No. 3040556 — Form 2-17-85

Simplex Security Systems, Inc.

FRONT AND MAIN STS., COLLINSVILLE, CT 06022 • (203) 693-8391 [illegible]

Lenox said, "[The university] did not consider contacting the university locksmith on his expertise. I had originally told them years ago when the Simplex locks were first introduced...not to use [the locks] in the dormitories." Not only are they being used in the dormitories, but the university is considering purchasing 1500 more for additional rooms.

The illusion of security Simplex is portraying with misleading advertising is that Simplex locks are just as secure, if not more secure, than key locks. The result of this myth is that many businesses, institutions, and homeowners confidently use Simplex locks as the only lock source despite the fact that the locks are inherently insecure. Even when locksmiths are consulted, we have found that they simply perpetuate the illusion of security by claiming that Simplex locks are "top of the line" and that "even the Department of Defense uses them." Nowhere is it mentioned that Simplex locks should never be used as the only lock source. Even worse, Simplex is now aggressively pursuing the homeowner market with their new "residential" 6000 series. These new locks employ the same insecure mechanism, and are being marketed as primary locks.

Realistically, Simplex locks are more of a convenience lock than anything else. They are convenient because they do not require keys and the combinations are easily changed. However, this convenience backfires when it comes to security. These locks are so convenient that people tend not to use other locks that may also be present on the door.

For those organizations currently using Simplex locks, we recommend following the guidelines of the DoD Security Manual: the locks may be used as the sole lock source *only during working hours.* For home or private use, we strongly advise that consumers use these locks in conjunction with a key lock and never as the sole means of security.

Hacking Simplex Locks

In this issue is a list of all possible combinations for Simplex locks. We have divided the list into four groups according to how many pushbuttons are used. The numbers listed in parentheses refer to pushbuttons that must be pressed together. If you find that none of the combinations appear to open the lock, then it may be a rare instance of a half-step code. In this case, only the last number (or numbers if they are in parentheses) should be pressed in *halfway* and held while the knob or latch is turned. Slowly press in the pushbutton(s) until you feel pressure. If you hear a click then you have pushed the buttons in too far. If all of this sounds complicated, then you are beginning to understand why it is that Simplex does not recommend the use of half-step codes, and subsequently why half step codes are virtually never used.

Simplex locks come in many different shapes, sizes, and colors. However, the two models that you will most likely see are the 900 and the 1000 series. The characteristic features of the 900 series are five black buttons spaced in a circular fashion on a round, metallic cylinder. In addition, the 900 series utilizes a latch instead of a doorknob. The 1000 series is much larger, with five (usually metallic) pushbuttons spaced vertically on a rectangular metal chassis. Unlike the 900 series, the 1000 has a doorknob.

We suggest that novices attempt their first hack on a Simplex 900 model. If the latch is located below the buttons, then the procedure is as follows: 1) turn the latch counterclockwise to reset the lock; 2) enter a combination from the list; 3) turn the latch clockwise to open. If the latch is located above the buttons then simply reverse the procedure. Make sure that you reset the lock after each try.

To hack a 1000 model, simply enter a combination from the list and turn the knob clockwise. You will hear clicks as you turn the knob, indicating that the lock has been reset. It is sometimes difficult to tell when you have cracked a 1000 model by simply turning the knob. When you do get the correct code, you will hear a distinctive click and feel less pressure as you turn the knob.

You will find that turning the latch on a 900 model requires less wrist motion and makes much less noise than turning the knob on a 1000 model. These details seem trivial until you realize that you may have to turn the latch or doorknob a few hundred times before you crack the lock.

We cannot stress enough how much easier it is when you know the range. For instance, if you know that only three digits are being used, then you do not have to waste time trying four digits. One way to find out the range is to stand nearby while someone punches in the code. You will hear distinctive clicks which will give you an idea of the range. If you cannot stand nearby then try hiding a voice activated tape recorder near the door. The tape recorder will remain off until someone comes up to punch in the code. You can then retrieve the recorder later at your convenience and listen for the telltale clicks. We find that this method only works in quiet areas, such as the inside of a building. Another way to find out the range is to take a pencil eraser and carefully rub off a tiny bit of rubber on each of the pushbuttons. When someone comes to enter the combination, they will rub off the rubber on all of the pushbuttons that they use, while leaving telltale traces of rubber on the pushbuttons that they do not use. This method works particularly well because you eliminate pushbuttons, which drastically reduces the number of combinations that must be tried.

We find that certain ranges tend to be used more than others. Group B (three pushbuttons) tends to be used in "low security areas," while Groups C and D tend to be used in areas which seem like they should be more secure. We have never found a lock which uses a combination from Group A. For some reason, we find that the 1000 series mostly uses Group C (four pushbuttons). In addition, most combinations tend to be "doubles," which require at least two of the pushbuttons to be pressed together. When you decide on a particular range to start with, try the doubles first. For instance, try "(12) 3 4 5" before you try "1 2 3 4 5." We have never found a lock which uses a triple, quadruple, or all five pushbuttons pressed at the same time.

Although we are providing a list of all the possible combinations, you may find it useful to invest some time and record these codes onto cassette. This makes it much easier for one person to hack a Simplex lock because he does not have to hold the codes in one hand while hacking, nor cross out the codes to keep his place. A walkman also looks far less conspicuous than sheets of paper filled with numbers. The only drawback to using a walkman is that the person hacking will not be able to hear anyone coming from a distance. We find it easier to hack Simplex locks in small groups, so that each person can take turns, and everyone has their ears open.

Finally, it is always good to take a few lucky shots before you initiate a brute force hack. Always try the default combination "(24) 3" before you try anything else. Above all, *don't give up!* Even if you do not get the combination in ten minutes, you are still that much closer to figuring it out. We recommend that you do not stress yourself out trying every combination in one shot. A few minutes a day will do just fine, and the thrill of achievement will be well worth the wait.

1085 POSSIBLE COMBINATIONS DIVIDED INTO FOUR GROUPS

(Numbers in parentheses should be pressed together)

GROUP A:
39

1
2
3
4
5
1 2
1 3
1 4
1 5
2 1
2 3
2 4
2 5
3 1
3 2
3 4
3 5
4 1
4 2
4 3
4 5
5 1
5 2
5 3
5 4
(12)
(13)
(14)
(15)
(23)
(24)
(25)
(34)
(35)
(45)
(51)
(52)
(53)
(54)

GROUP B:
130

1 2 3
1 2 4
1 2 5
1 3 2
1 3 4
1 3 5
1 4 2
1 4 3
1 4 5
1 5 2
1 5 3
1 5 4
2 1 3
2 1 4
2 1 5
2 3 1
2 3 4
2 3 5
2 4 1
2 4 3
2 4 5
2 5 1
2 5 3
2 5 4
3 1 2
3 1 4
3 1 5
3 2 1
3 2 4
3 2 5
3 4 1
3 4 2
3 4 5
3 5 1
3 5 2
3 5 4
4 1 2
4 1 3
4 1 5
4 2 1
4 2 3
4 2 5
4 3 1
4 3 2
4 3 5
4 5 1
4 5 2
4 5 3
5 1 2
5 1 3
5 1 4
5 2 1
5 2 3
5 2 4
5 3 1
5 3 2
5 3 4
5 4 1
5 4 2
5 4 3
(12) 3
(12) 4
(12) 5
(13) 2
(13) 4
(13) 5
(14) 2
(14) 3
(14) 5
(15) 2
(15) 3
(15) 4
(23) 1
(23) 4
(23) 5
(24) 1
(24) 3
(24) 5
(25) 1
(25) 3
(25) 4
(34) 1
(34) 2
(34) 5
(35) 1
(35) 2
(35) 4
(45) 1
(45) 2
(45) 3
3 (12)
4 (12)
5 (12)
2 (13)
4 (13)
5 (13)
2 (14)
3 (14)
5 (14)
2 (15)
3 (15)
4 (15)
1 (23)
4 (23)
5 (23)
1 (24)
3 (24)
5 (24)
1 (25)
3 (25)
4 (25)
1 (34)
2 (34)
5 (34)
1 (35)
2 (35)
4 (35)
1 (45)
2 (45)
3 (45)
(123)
(124)
(125)
(134)
(135)
(145)
(234)
(235)
(245)
(345)

GROUP C:
375

1 2 3 4
1 2 3 5
1 2 4 3
1 2 4 5
1 2 5 3
1 2 5 4
1 3 2 4
1 3 2 5
1 3 4 2
1 3 4 5
1 3 5 2
1 3 5 4
1 4 2 3
1 4 2 5
1 4 3 2
1 4 3 5
1 4 5 2
1 4 5 3
1 5 2 3
1 5 2 4
1 5 3 2
1 5 3 4
1 5 4 2
1 5 4 3
2 1 3 4
2 1 3 5
2 1 4 3
2 1 4 5
2 1 5 3
2 1 5 4
2 3 1 4
2 3 1 5
2 3 4 1
2 3 4 5
2 3 5 1
2 3 5 4
2 4 1 3
2 4 1 5
2 4 3 1
2 4 3 5
2 4 5 1
2 4 5 3
2 5 1 3
2 5 1 4
2 5 3 1
2 5 3 4
2 5 4 1
2 5 4 3
3 1 2 4
3 1 2 5
3 1 4 2
3 1 4 5
3 1 5 2
3 1 5 4
3 2 1 4
3 2 1 5
3 2 4 1
3 2 4 5
3 2 5 1
3 2 5 4
3 4 1 2
3 4 1 5
3 4 2 1
3 4 2 5
3 4 5 1
3 4 5 2
3 5 1 2
3 5 1 4
3 5 2 1
3 5 2 4
3 5 4 1
3 5 4 2
4 1 2 3
4 1 2 5
4 1 3 2
4 1 3 5
4 1 5 2
4 1 5 3
4 2 1 3
4 2 1 5
4 2 3 1
4 2 3 5
4 2 5 1
4 2 5 3
4 3 1 2
4 3 1 5
4 3 2 1
4 3 2 5
4 3 5 1
4 3 5 2
4 5 1 2
4 5 1 3
4 5 2 1
4 5 2 3
4 5 3 1
4 5 3 2
5 1 2 3
5 1 2 4
5 1 3 2
5 1 3 4
5 1 4 2
5 1 4 3
5 2 1 3
5 2 1 4
5 2 3 1
5 2 3 4
5 2 4 1
5 2 4 3
5 3 1 2
5 3 1 4
5 3 2 1
5 3 2 4
5 3 4 1
5 3 4 2
5 4 1 2
5 4 1 3
5 4 2 1
5 4 2 3
5 4 3 1
5 4 3 2
(12) 3 4
(12) 3 5
(12) 4 3
(12) 4 5
(12) 5 3
(12) 5 4
(13) 2 4
(13) 2 5
(13) 4 2
(13) 4 5
(13) 5 2
(13) 5 4
(14) 2 3
(14) 2 5
(14) 3 2
(14) 3 5
(14) 5 2
(14) 5 3
(15) 2 3
(15) 2 4
(15) 3 2
(15) 3 4
(15) 4 2
(15) 4 3
(23) 1 4
(23) 1 5
(23) 4 1
(23) 4 5
(23) 5 1
(23) 5 4
(24) 1 3
(24) 1 5
(24) 3 1
(24) 3 5
(24) 5 1
(24) 5 3
(25) 1 3
(25) 1 4
(25) 3 1
(25) 3 4
(25) 4 1
(25) 4 3
(34) 1 2
(34) 1 5
(34) 2 1
(34) 2 5
(34) 5 1
(34) 5 2
(35) 1 2
(35) 1 4
(35) 2 1
(35) 2 4
(35) 4 1
(35) 4 2
(45) 1 2
(45) 1 3
(45) 2 1
(45) 2 3
(45) 3 1
(45) 3 2
3 (12) 4
3 (12) 5
4 (12) 3
4 (12) 5
5 (12) 3
5 (12) 4
2 (13) 4
2 (13) 5
4 (13) 2
4 (13) 5
5 (13) 2
5 (13) 4
2 (14) 3
2 (14) 5
3 (14) 2
3 (14) 5
5 (14) 2
5 (14) 3
2 (15) 3
2 (15) 4
3 (15) 2
3 (15) 4
4 (15) 2
4 (15) 3
1 (23) 4
1 (23) 5
4 (23) 1
4 (23) 5
5 (23) 1
5 (23) 4
1 (24) 3
1 (24) 5
3 (24) 1
3 (24) 5
5 (24) 1
5 (24) 3
1 (25) 3
1 (25) 4
3 (25) 1
3 (25) 4
4 (25) 1
4 (25) 3
1 (34) 2
1 (34) 5
2 (34) 1
2 (34) 5
5 (34) 1
5 (34) 2
1 (35) 2
1 (35) 4
2 (35) 1
2 (35) 4
4 (35) 1
4 (35) 2
1 (45) 2
1 (45) 3
2 (45) 1
2 (45) 3
3 (45) 1
3 (45) 2
3 4 (12)
3 5 (12)
4 3 (12)
4 5 (12)
5 3 (12)
5 4 (12)
2 4 (13)
2 5 (13)
4 2 (13)
4 5 (13)
5 2 (13)
5 4 (13)
2 3 (14)
2 5 (14)
3 2 (14)
3 5 (14)
5 2 (14)
5 3 (14)
2 3 (15)
2 4 (15)
3 2 (15)
3 4 (15)
4 2 (15)
4 3 (15)
1 4 (23)
1 5 (23)
4 1 (23)
4 5 (23)
5 1 (23)
5 4 (23)
1 3 (24)
1 5 (24)
3 1 (24)
3 5 (24)
5 1 (24)
5 3 (24)
1 3 (25)
1 4 (25)
3 1 (25)
3 4 (25)
4 1 (25)
4 3 (25)
1 2 (34)
1 5 (34)
2 1 (34)
2 5 (34)
5 1 (34)
5 2 (34)
1 2 (35)
1 4 (35)
2 1 (35)
2 4 (35)
4 1 (35)
4 2 (35)
1 2 (45)
1 3 (45)
2 1 (45)
2 3 (45)
3 1 (45)
3 2 (45)
(12) (34)
(12) (35)
(12) (45)
(13) (24)
(13) (25)
(13) (45)
(14) (23)
(14) (25)
(14) (35)
(15) (23)
(15) (24)
(15) (34)
(23) (14)
(23) (15)
(23) (45)
(24) (13)
(24) (15)
(24) (35)
(25) (13)
(25) (14)
(25) (34)
(34) (12)
(34) (15)
(34) (25)
(35) (12)
(35) (14)
(35) (24)
(45) (12)
(45) (13)
(45) (23)
(123) 4
(123) 5
(124) 3
(124) 5
(125) 3
(125) 4
(134) 2
(134) 5
(135) 2
(135) 4
(145) 2
(145) 3
(234) 1
(234) 5
(235) 1
(235) 4
(245) 1
(245) 3
(345) 1
(345) 2
4 (123)
5 (123)
3 (124)
5 (124)
3 (125)
4 (125)
2 (134)
5 (134)
2 (135)
4 (135)

(continued on page 45)

The Hacker Video

Over the summer, military computer systems in the United States were accessed by Dutch hackers. One of the episodes was captured on videotape by *2600*, portions of which were shown on a recent nationwide television show. Most of it, however, has never been seen. We are releasing this videotape to the public so that more people will witness just how shamefully easy it is to get access to military computers.

The intrusion took place in late July of this year. The purpose of this demonstration was to show just how easy it really was. Great care was taken to ensure that no damage or alteration of data occurred on this particular system. No military secrets were taken and no files were saved to a disk by the hackers. What is frightening is that nobody knows who else has access to this information or what their motivations might be. This is a warning that cannot be taken lightly.

Explanation of the Videotape

The tape opens with some background shots of the hacker site in Amsterdam. Basically, it's a group of about five people in their twenties gathered together to match wits and play with computers.

Through a local phone number, a connection is made to the Internet. This network ties together schools, corporations, and government installations around the world. By connecting from one machine on the Internet to another, you can use two or more computers at once, without a noticeable loss of speed.

```
telnet 192.67.67.20
```

Using a program called "telnet", the hackers connect to the Defense Data Network Information Center. (Telnet enables a user to actually login to systems all over the world.) In this case, the particular address is "192.67.67.20", a computer which requires no password and is open to everyone. (The address has since been changed to 192.112.36.5.) It is a clearinghouse of information about various systems and their users.

The hackers are met with a "Whois:" prompt. The computer is asking them who they want to have checked out. The hackers type "army.mil", indicating any computer on the military network that has the word "army" in its address. The computer spits out over one thousand computer names and addresses.

A computer named "tracer.army.mil" at address 192.33.5.135 is chosen at random. (This computer is believed to be located at Los Alamos, but this has not been confirmed.) The hackers then begin to try default passwords, like "guest", "public", "uucp", etc. None of these work.

```
ftp -n tracer.army.mil
```

The next line of attack is the ftp command. By using ftp (file transfer protocol), anyone can copy files from one system to another. Ftp is similar to telnet in that it connects to systems all over the world. But while telnet is used to login to systems, ftp is only used to transfer files. In addition, it is not necessary to have accounts on more than one machine in order to use ftp.

The way it works is as follows: a user logs into a machine on the Internet. Using ftp, he connects to another machine, which then asks him for a user name. By typing "anonymous", the user is granted limited access to the machine. The purpose of this is so that public files can be made available without having to give out accounts to everyone needing access.

```
quote user ftp
quote cwd ~root
quote pass ftp
```

But this version of ftp has at least one major bug in its software. By issuing the above commands, the user is not only able to gain access to the machine, but change his directory (location) on the system to the root directory. (Root is the most powerful account on the system.) So instead of being able to look at a limited number of files on the system, the anonymous user is now able to look at anything. In addition, the hackers can also change anything, albeit with great difficulty. This is because the hackers are not actually logged into the system. They are still confined to working within the framework of the ftp program.

At this stage, while the hackers can read and alter any bit of information on this military system, they cannot run any programs. Also, they cannot actually login to the system. But this doesn't remain a problem for very long.

```
get /etc/passwd
exit ftp and modify passwd file on
home system
```

Since ftp allows users to copy files, the hackers choose to copy the password file (known as "/etc/passwd"). This file contains a list of every user on the system along with their encrypted password. It is virtually impossible to actually decrypt these passwords, which is why the file is readable by any user on the system. (It is not supposed to be readable through ftp, however.) Ordinarily, copying this file would not be very significant. However, once the hackers have the file copied to their home system, they carefully insert another user into it. Since the system believes they have certain privileges, it allows them to replace the old version of the password file with their new version.

The user name they create is "dquayle". In the field where the encrypted password would be is nothing. This means there is no password for Dan Quayle's newly created account. Hence they do not have to worry about decrypting it. The hackers apparently had intended to give dquayle root privileges by inputting the appropriate values for his account. But a careful look at the videotape will show that dquayle was not given any special privileges.

```
ftp -n tracer.army.mil
quote user ftp
quote cwd ~root
quote pass ftp
put /etc/passwd
exit ftp
```

The hackers repeat the first series

of steps (henceforth known as the "ftp bug") to once again get root privileges. The original passwd file is now replaced with the modified version containing the fictitious user "dquayle".

```
telnet tracer.army.mil
```

The hackers reconnect to the military system, which asks for a username. The hackers type in "dquayle". Access is granted without a password.

But root access is not granted. Instead, a warning is printed on the screen indicating that the terminal is "not a secure device". In many cases, the system will not allow root access to anyone coming in from the outside. This was what originally appeared to have happened. However, as mentioned earlier, dquayle had no special privileges, so the system never even tried to access root. Either way, it would seem that the hackers' ultimate goal has been thwarted.

```
exit telnet and modify passwd file
on home system
ftp -n tracer.army.mil
quote user ftp
quote cwd ~root
quote pass ftp
put /etc/passwd
exit ftp
```

Instead of giving up, the hackers go back to their copy of the password file. They make another account, this time with root privileges and no password. This account they call "toor", the word root backwards. They once again make use of the ftp bug to "put" the new password file on the system.

```
telnet tracer.army.mil
su toor
```

Using telnet, the hackers once again login as dquayle. This time, after the warning is issued, they issue a two letter command ("su") followed by their new user ("toor"). The su command allows a user to switch to the identity of another user while logged in. It saves the trouble of hanging up and calling back into the system and is useful if someone has two accounts or if two users are sharing a terminal. In this particular case, the hope is that the su command will not check to see if the call was coming from outside.

No password is requested since none was entered into the toor account. A single "#" on the screen tells the hackers that their mission has succeeded. That symbol indicates true root access. The su command granted them root access even though they were coming in from the outside. Since they were already logged onto the system, su assumed they were legitimate. This military computer system (tracer.army.mil) is now completely under the hackers' control.

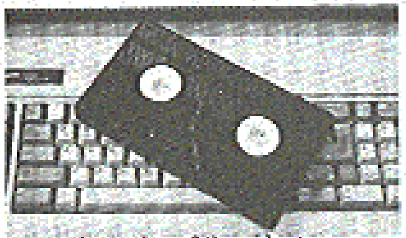
The rest of the night is spent looking for interesting bits of data to prove beyond a doubt that this is not a system for just anyone to be in. The next day, some of the data is scrolled through. Among the more interesting pieces is a memo from the Counterterrorism Officer dated January 15, 1991 (the deadline day for Iraqi troops to be withdrawn from Kuwait) discussing security issues. Clearly, this is sensitive information.

How Passwords Are Guessed

The final part of the tape illustrates a password hacker program. Using the aforementioned password file, the program comes up with the most commonly used passwords. Instead of decrypting the passwords in the password file, it encrypts the possible passwords (the encryption algorithm is standard) and then compares them to the actual passwords. If they match, then a password has been found. In the example shown (from a different system), many passwords are found in this manner.

Why We Are Exposing This

The hackers responsible for this are not interested in military secrets. But they do recognize the importance and value of the information that is stored on such computers. The fact of the matter is that if these gaping security holes are not openly exposed, they will never get fixed. Ironically, the bug that was used in this particular case is a fairly old one that has been fixed on most systems. Why it still existed on a military system is beyond us. But we do know that this is only one system and only one bug.



A portion of the videotape

Corporate computer systems also continue to operate with security holes. As hackers, we are concerned with the lack of safeguards that are being placed upon sensitive data. In addition to military data, much information about individual people continues to be sloppily managed. Our credit ratings, telephone records, banking information, and computerized files of all sorts are open to scrutiny for anyone who can gain access.

We should stress that the vast majority of unauthorized access does not involve computer hackers. Since we have no ulterior motives, other than the quest for knowledge, we openly reveal whatever we find out. Unfortunately, this often results in our being blamed for the problem itself — confusing the messenger with the message. In reality, there are countless instances of employees invading the privacy of individuals by accessing credit files or billing information that they have no business seeing. Since this information is so easy for them to get ahold of, there is virtually no way of their being detected. And, even if they were detected, they aren't really breaking any laws.

Add to this the increasing fragility of our modern technology as computers become dependent upon other computers and it becomes evident that serious problems, even catastrophes, lie ahead. The actions of computer hackers are, at worst, an annoyance to some rather powerful people. Were we not to expose the flaws in the system, they would still be there and they would most definitely be abused.

We will send you a VHS copy for $10 or 3 blank 120 tapes.

protecting your ssn

by Chris Hibbert
Computer Professionals for
Social Responsibility

Many people are concerned about the number of organizations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being treated as just a number.

Unfortunately, I can't offer any hope about the dehumanizing effects of identifying you with your numbers. I can try to help you keep your Social Security Number from being used as a tool in the invasion of your privacy.

Surprisingly, government agencies are reasonably easy to deal with; private organizations are much more troublesome. Federal law restricts the agencies at all levels of government that can demand your number and a fairly complete disclosure is required even if its use is voluntary. There are no comparable laws restricting the uses non-government organizations can make of it, or compelling them to tell you anything about their plans. With private institutions, your main recourse is refusing to do business with anyone whose terms you don't like.

Short History

Social Security Numbers were introduced by the Social Security Act of 1935. They were originally intended to be used only by the Social Security program, and public assurances were given at the time that use would be strictly limited. In 1943 Roosevelt signed Executive Order 9397 which required federal agencies to use the number when creating new record-keeping systems. In 1961 the IRS began to use it as a taxpayer ID number. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their databases and required disclosures (detailed below) when government agencies request the number. Agencies which were already using SSN as an identifier were allowed to continue using it. The Tax Reform Act of 1976 gave authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. The Privacy Protection Study Commission of 1977 recommended that the Executive Order be repealed after some agencies referred to it as their authorization to use SSNs. I don't know whether it was repealed, but that practice has stopped.

The Privacy Act of 1974 (5 USC 552a) requires that any federal, state, or local government agency that requests your Social Security Number has to tell you three things:

1: Whether disclosure of your Social Security Number is required or optional.

2: What law authorizes them to ask for your Social Security Number.

3: How your Social Security Number will be used if you give it to them.

In addition, the Act says that only Federal law can make use of the Social Security Number mandatory. So anytime you're dealing with a government institution and you're asked for your Social Security Number, just look for the Privacy Act Statement. If there isn't one, complain and don't give your number. If the statement is present, read it. If it says giving your Social Security Number is voluntary, you'll have to decide for yourself whether to fill in the number.

Private Organizations

The guidelines for dealing with non-governmental institutions are much more tenuous. Most of the time private organizations that request your Social Security Number can get by quite well without your number, and if you can find the right person to negotiate with, they'll willingly admit it. The problem is finding that right person. The person behind the counter is often told no more than "get the customers to fill out the form completely."

Most of the time, you can convince them to use some other number. Usually the simplest way to refuse to give your Social Security Number is simply to leave the appropriate space blank. One of the times when this isn't a strong enough statement of your desire to conceal your number is when dealing with institutions which have direct contact with your employer. Most employers have no policy against revealing your Social Security Number; they usually believe the omission was an unintentional slip.

Lenders and Borrowers

Banks and credit card issuers are required by the IRS to report the SSNs of account holders to whom they pay interest or when they charge interest and report it to the IRS. If you don't tell them your number you will probably either be refused an account or be charged a penalty such as withholding of taxes on your interest.

Insurers, Hospitals, Doctors

No laws require medical service providers to use your Social Security Number as an ID number (except for Medicare, Medicaid, etc.). They often use it because it's convenient or because your employer uses it to certify employees to its group health plan. In the latter case, you have to get your employer to change their policies. Often, the people who work in personnel assume that the employer or insurance company requires use of the SSN when that's not really the case. When my current employer asked for my SSN for an insurance form, I asked them to try to find out if they had to use it. After a week they reported that the insurance company had gone along with my request and told me what number to use. Blood banks also ask for the number but are willing to do without if pressed on the issue. After I asked politely and persistently, the blood bank I go to agreed that they didn't have any use for the number, and is in the process of teaching their receptionists not to request the number.

Why Use of Social Security Numbers is a Problem

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't at all secure; if someone makes up a nine-digit number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number: to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants); or to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally giving a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers. (One is given below.)

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whichever record it shows up on. When it happens accidentally, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

What You Can Do to Protect Your Number

If despite your having written "refused" in the box for Social Security Number, it still shows up on the forms someone sends back to you (or worse, on the ID card they issue), your recourse is to write letters or make phone calls. Start politely, explaining your position and expecting them to understand and cooperate. If that doesn't work, there are several more things to try:

1) Talk to people higher up in the organization. This often works simply because the organization has a standard way of dealing with requests not to use the SSN, and the first person you deal with just hasn't been around long enough to know what it is.

2) Enlist the aid of your employer. You have to decide whether talking to someone in personnel, and possibly trying to change corporate policy, is going to get back to your supervisor and affect your job.

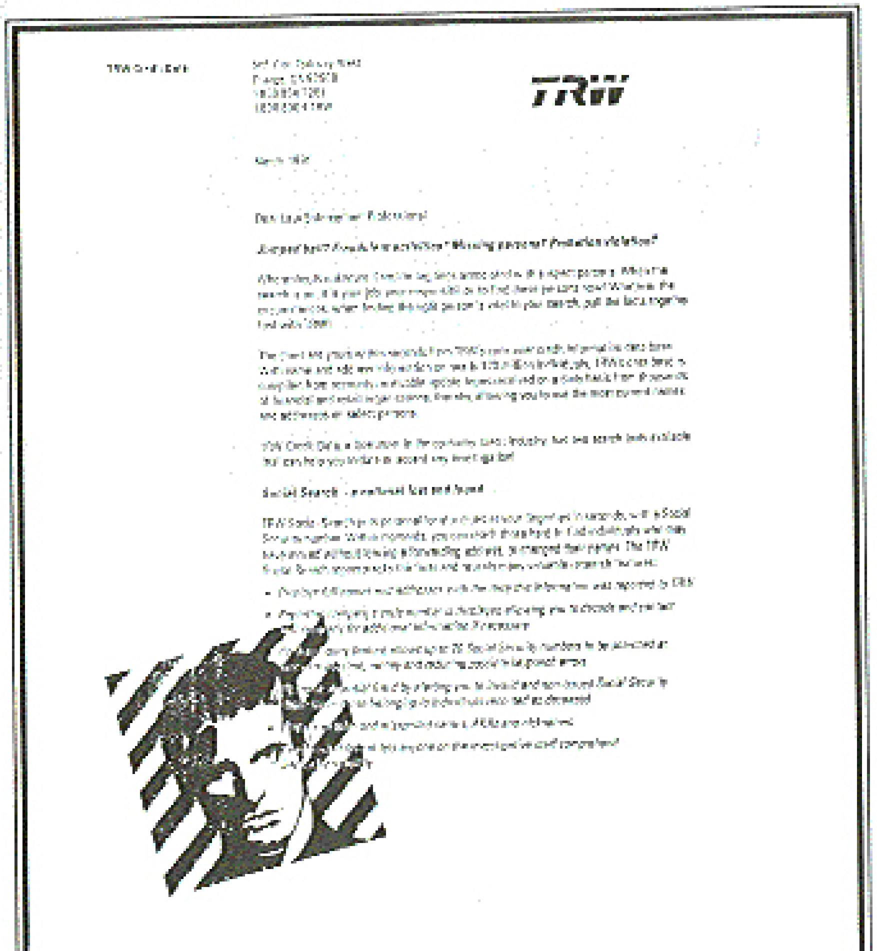
3) Threaten to complain to a consumer affairs bureau. Most newspapers can get a quick response. Some cities, counties, and states also have programs that might be able to help.

4) Tell them you'll take your business elsewhere (and follow through if they don't cooperate).

5) If it's a case where you've gotten service already, but someone insists that you have to provide your number in order to have a continuing relationship, you can choose to ignore the request in hopes that they'll forget or find another solution before you get tired of the interruption.

If someone absolutely insists on getting your Social Security Number, you may want to give a fake number. There is no legal penalty as long as you're not doing it to get something from a government agency or to commit fraud. There are a few good choices for "anonymous" numbers. Making one up at random is a bad idea, as it may coincide with someone's real number and cause them some amount of grief. It's better to use a number like 078-05-1120, which was printed on "sample" cards inserted in thousands of new wallets sold in the 40's and 50's. It's been used so widely that both the IRS and SSA recognize it immediately as bogus, while most clerks haven't heard of it. It's also safe to invent a number that has only zeros in one of the fields. The Social Security Administration never issues numbers with this pattern. They also recommend that people showing Social Security cards in advertisements use numbers in the range 987-65-4320 through 987-65-4329.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.



TRW

[illegible]

Social Search [illegible]

[illegible]

This kind of thing goes on all the time. This is but one example.

COCOT NUMBERS
(Customer Owned Coin Operated Telephones)

WASHINGTON DC COCOTS
by The Dead Cow

202-362-5099 (12)
202-364-9936 (12)
202-966-4871 (3)
202-966-4356 (12)
202-244-2348 (3)
202-232-0488 (3)
202-463-1546 (3)
202-463-1547 (3)
202-296-5215 (3)
301-229-9802 (3)
301-652-4725 (3)

THESE PHONES ANSWER WITH A CARRIER TONE. (3) INDICATES A 300 BAUD CONNECTION, (12) A 1200 BAUD CONNECTION.

NEW ENGLAND COCOTS
by NB

Nearly all of these phones will answer with a synthesized voice that says "Thank you," plays four tones, and then waits for input. As far as we know, nobody has cracked this popular system yet.

MAINE

207-284-4548
207-363-9700
207-729-1104
207-761-0543
207-761-2939
207-761-7910
207-772-1540
207-772-5807
207-772-9145
207-772-9160
207-772-9173
207-772-9216
207-772-9327
207-772-9336
207-772-9366
207-772-9379
207-772-9382
207-772-9413
207-772-9439
207-772-9469
207-772-9470
207-772-9482
207-772-9483
207-772-9487
207-772-9493
207-773-0414
207-773-1082
207-773-4629
207-773-9104
207-773-9157
207-773-9111
207-773-9117
207-773-9179
207-773-9261
207-773-9121
207-773-9337
207-773-9330
207-773-9347
207-773-9348
207-773-9380
207-773-9426
207-773-9477
207-773-9479
207-774-5348
207-775-5119
207-775-5180
207-775-5339
207-775-5729
207-775-5806
207-777-1517
207-797-9813
207-797-9816
207-799-7030
207-799-7374
207-828-1261
207-854-8958
207-854-8987
207-854-9054
207-871-9391
207-874-0904
207-878-2317
207-879-0625
207-883-9314
207-883-9355
207-892-1797
207-892-1798

RHODE ISLAND

401-231-1870
401-231-2560
401-231-3430
401-231-3880
401-231-3961
401-231-8323
401-231-8850
401-231-9257
401-231-9612
401-231-9614
401-231-9619
401-231-9641
401-231-9642
401-231-9689
401-232-0273
401-232-6036
401-232-6377
401-232-7243
401-232-7939
401-233-0334
401-245-2359
401-245-9330
401-245-9344
401-245-9424
401-253-1880
401-253-9256
401-253-9680
401-253-9700
401-253-9786
401-253-9815
401-254-0816
401-254-1370
401-272-1570
401-272-6396
401-272-6739
401-272-6904
401-272-9239
401-273-0980
401-273-1671
401-273-1958
401-273-1951
401-273-1956
401-273-1957
401-273-7940
401-273-7891
401-273-7897
401-273-9331
401-274-1059
401-274-8706
401-276-9545
401-295-1247
401-295-1569
401-295-7701
401-331-1171
401-331-1660
401-331-2320
401-331-2056
401-331-4280
401-331-4521
401-331-6549
401-331-8626
401-331-8967
401-331-9073
401-333-4198
401-333-4366
401-333-9803
401-334-3620
401-348-0287
401-348-9007
401-351-0147
401-351-5060
401-351-5080
401-351-6241
401-351-7080
401-353-6612
401-353-9736
401-364-8673
401-377-4750
401-377-7001
401-397-3570
401-421-0979
401-421-1032
401-421-4543
401-421-5563
401-421-8883
401-421-8831
401-421-9270
401-421-9360
401-421-9706
401-431-9347
401-431-4020
401-434-8540
401-434-7178
401-434-7055
401-434-8559
401-434-9611
401-434-9640
401-434-8790
401-434-9802
401-435-4380
401-437-9075
401-438-1540
401-438-2158
401-438-6856
401-438-9099
401-453-4025
401-453-4826
401-453-4839
401-453-6206
401-454-0425
401-454-0430
401-454-0490
401-454-0517
401-454-0826
401-454-1307
401-454-4077
401-454-7414
401-454-8409
401-454-8459
401-454-8579
401-455-0909
401-455-2300
401-461-8074
401-461-8135
401-461-8541
401-463-6058
401-463-9619
401-467-0510
401-467-8904
401-521-5219
401-567-0046
401-568-2425
401-568-6500
401-568-7106
401-568-7119
401-568-7127
401-568-8540
401-596-2040
401-596-4620
401-596-6863
401-596-9049
401-598-8131
401-598-8174
401-596-9391
401-596-9546
401-621-1178
401-621-7348
401-621-2891
401-621-5197
401-621-5870
401-621-7886
401-621-8015
401-621-8017
401-621-8030
401-621-8033
401-621-8038
401-621-8039
401-621-8057
401-621-8058
401-621-8082
401-621-8120
401-621-8140
401-621-8151
401-621-8166
401-621-8186
401-621-8202
401-621-8213
401-621-8259
401-621-8318
401-621-8359
401-621-8377
401-621-8401
401-621-8407
401-621-8424
401-621-8463
401-621-8484
401-621-8523
401-621-8594
401-621-8618
401-621-8644
401-621-8646
401-621-8655
401-621-8661
401-621-8663
401-621-8664
401-621-8671
401-621-8759
401-621-8760
401-621-8762
401-621-8771
401-621-8774
401-621-8798
401-621-8802
401-621-8805
401-621-8807
401-621-8811
401-621-8813
401-621-8821
401-621-8836
401-621-8807
401-621-8828
401-621-8844
401-621-8858
401-621-8926
401-621-8928
401-621-8933
401-621-8945
401-621-8961
401-621-8962
401-621-8953
401-621-9017
401-621-9022
401-621-9031
401-621-9036
401-621-9043
401-621-9066
401-621-9077
401-621-9067
401-621-9150
401-621-9162
401-621-9166
401-621-9185
401-621-9201
401-621-9263
401-621-9334
401-621-9348
401-621-9423
401-621-9470
401-621-9510
401-621-9560
401-621-9701
401-621-9714
401-621-9727
401-621-9723
401-621-9744
401-621-9753
401-621-9842
401-621-9870
401-621-9878
401-621-9883
401-621-9885
401-621-9956
401-624-2967
401-624-2948
401-647-3811
401-647-3080
401-647-6042
401-683-1661
401-683-1766
401-683-3506
401-683-3858
401-683-4626
401-683-6889
401-683-8062
401-683-9854
401-683-9984
401-724-3240
401-724-3260
401-725-6940
401-725-8260
401-725-8889
401-725-8967
401-725-8966
401-726-8580
401-726-5627
401-726-5710
401-726-6901
401-726-6641
401-726-8782
401-726-8833
401-726-0056
401-726-8839
401-726-9011
401-726-9104
401-726-9138
401-726-9187
401-726-9226
401-726-9268
401-726-9263
401-726-9370
401-726-9411
401-726-9478
401-726-9519
401-726-9522
401-726-9660
401-726-9663
401-726-9867
401-727-0690
401-728-5580
401-732-0670
401-732-8619
401-732-8923
401-732-9190
401-737-2745
401-737-5448
401-737-8451
401-737-8653
401-737-9506
401-737-9616
401-737-9646
401-737-9689
401-737-9706
401-737-9732
401-737-9746
401-737-9844
401-737-9045
401-737-9873
401-738-0951
401-738-6033
401-738-1446
401-738-2046
401-738-3420
401-738-9700
401-738-9721
401-738-9734
401-738-9783
401-739-9806
401-751-5790
401-751-6943
401-751-7076
401-751-7259
401-751-7242
401-751-7766
401-751-7267
401-751-8475
401-762-0625
401-762-1367
401-762-2946
401-762-2977
401-762-4358
401-762-9333
401-762-9414
401-762-9428
401-762-9440
401-762-9445
401-762-9448
401-762-9467
401-762-9489
401-762-9519
401-762-9522
401-762-9523
401-762-9556

401-762-9574
401-762-9575
401-762-9589
401-762-9598
401-762-9671
401-762-9702
401-762-9706
401-762-9721
401-762-9737
401-762-9845
401-762-9899
401-765-7614
401-765-8112
401-765-8149
401-765-0652
401-766-3321
401-766-9281
401-769-0673
401-769-2159
401-769-3008
401-769-3955
401-769-8791
401-769-8796
401-769-9073
401-781-8766
401-781-8942
401-782-2506
401-782-4380
401-782-6408
401-783-1018
401-783-1065
401-783-1098
401-783-7613
401-783-7614
401-783-7630
401-783-7631
401-783-7637
401-789-8176
401-789-7242
401-789-8440
401-789-8531
401-789-8561
401-789-8563
401-789-9606
401-821-0399
401-821-0695
401-821-2645
401-821-7632
401-821-8675
401-821-8773
401-821-9610
401-821-9627
401-821-9639
401-821-9647
401-821-9687
401-821-9690
401-821-9725
401-821-9738
401-821-9819
401-821-9883
401-821-9896
401-823-0226
401-823-1297
401-823-1545
401-823-7575
401-828-3610
401-828-9510
401-828-9611
401-828-9720
401-828-9935
401-828-9972
401-831-0379
401-831-5667
401-831-9118
401-831-9120
401-831-9147
401-831-9176
401-831-9198
401-831-9204
401-831-9231
401-831-9233
401-831-9235
401-831-9259
401-831-9260
401-831-9273
401-831-9306
401-831-9338
401-831-9343
401-831-9345
401-831-9346
401-831-9349
401-831-9455
401-831-9504
401-831-9509
401-831-9518
401-831-9551
401-831-9724
401-831-9736
401-831-9739
401-831-9759
401-831-9841
401-831-9860
401-831-9871
401-831-9896
401-846-0335
401-846-0712
401-846-2510
401-846-3659
401-846-4769
401-846-4980
401-846-5644
401-846-6790
401-846-7119
401-846-7200
401-846-7540
401-846-8122
401-846-8522
401-846-8545
401-846-8569
401-846-8670
401-846-8714
401-846-8720
401-846-8730
401-846-8731
401-846-8732
401-846-8736
401-846-8737
401-846-8738
401-846-8742
401-846-8752
401-846-8787
401-846-8789
401-846-8792
401-846-8794
401-846-8803
401-846-8830
401-846-8831
401-846-8868
401-846-8874
401-846-8884
401-846-8846
401-846-8487
401-847-0504
401-847-2139
401-847-2465
401-847-8329
401-847-8338
401-847-9364
401-847-9368
401-847-9378
401-847-9379
401-847-9432
401-847-9441
401-847-9449
401-847-9500
401-847-9503
401-847-9504
401-847-9531
401-847-9558
401-847-9561
401-847-9630
401-847-9639
401-847-9641
401-847-9642
401-847-9667
401-847-9668
401-847-9698
401-847-9705
401-847-9720
401-847-9727
401-847-9726
401-847-9741
401-847-9744
401-847-9745
401-847-9747
401-847-9895
401-848-0259
401-848-0530
401-848-0722
401-849-0390
401-848-0916
401-849-2632
401-849-2712
401-849-5264
401-849-5709
401-849-8470
401-849-2900
401-849-2912
401-849-2913
401-849-2928
401-849-1251
401-849-1252
401-849-1256
401-849-1259
401-849-1908
401-849-1922
401-849-1923
401-849-1924
401-849-1929
401-849-1930
401-849-1931
401-849-1946
401-849-1947
401-849-1971
401-849-1977
401-849-1988
401-849-1995
401-849-1998
401-849-2128
401-849-2453
401-849-2636
401-849-5195
401-849-8842
401-849-8983
401-849-8985
401-849-8986
401-849-9721
401-861-1360
401-861-2144
401-861-2146
401-861-2149
401-861-2800
401-861-8535
401-884-3170
401-884-5435
401-884-8933
401-884-5776
401-884-8792
401-884-9810
401-884-9832
401-934-9936
401-934-9941
401-941-4790
401-941-9222
401-941-9424
401-941-9423
401-941-9430
401-941-9457
401-941-9487
401-941-9502
401-941-9529
401-941-9732
401-941-9745
401-941-9831
401-942-9518
401-942-9549
401-942-9562
401-942-9806
401-944-0796
401-944-4706
401-944-8714
401-944-8786
401-946-0594
401-946-0596
401-949-9918

MASSACHUSETTS

508-222-8727
508-222-9831
508-222-9061
508-252-4873
508-252-9359
508-278-7309
508-285-2913
508-295-9716
508-295-9858
508-295-9057
508-336-3478
508-336-4952
508-336-4937
508-336-7918
508-336-7928
508-336-7968
508-336-8321
508-336-8806
508-379-1047
508-384-7490
508-399-7812
508-399-8072
508-478-3262
508-478-6441
508-529-5849
508-559-0763
508-559-0619
508-583-6806
508-583-8646
508-586-4369
508-586-4379
508-636-5759
508-668-5527
508-668-6549
508-672-8057
508-672-9101
508-672-9138
508-672-9153
508-672-9174
508-672-9198
508-672-9251
508-672-9256
508-672-9298
508-672-9305
508-672-9307
508-672-9332
508-672-9335
508-672-9347
508-672-9374
508-672-9377
508-672-9392
508-672-9417
508-672-9429
508-672-9446
508-672-9448
508-672-9484
508-672-9498
508-672-9506
508-672-9535
508-672-9551
508-672-9556
508-672-9558
508-672-9593
508-672-9623
508-672-9729
508-673-1653
508-673-8376
508-674-4370
508-674-4776
508-674-4802
508-674-5413
508-674-6510
508-674-8338
508-674-8857
508-674-9176
508-675-0652
508-675-3136
508-675-9740
508-675-9533
508-676-0640
508-676-1122
508-676-3004
508-676-3341
508-676-5006
508-676-7611
508-676-7607
508-676-7617
508-676-7833
508-676-7919
508-676-7920
508-676-8960
508-677-0160
508-677-0343
508-677-1677
508-677-3603
508-677-3755
508-677-4758
508-677-4703
508-677-9379
508-678-1535
508-678-2929
508-678-3419
508-678-6905
508-678-9148
508-678-9320
508-678-9511
508-678-9517
508-678-9925
508-678-9930
508-678-9933
508-678-9842
508-678-9845
508-678-9856
508-678-9873
508-678-9874
508-678-9983
508-679-0972
508-679-0650
508-679-1471
508-679-2610
508-679-2617
508-679-2929
508-679-5036
508-679-5490
508-679-8001
508-679-9314
508-679-9489
508-679-9921
508-695-9019
508-695-9037
508-695-9042
508-695-9391
508-695-9920
508-695-9921
508-695-9910
508-695-9915
508-695-9923
508-699-8102
508-741-0300
508-741-3272
508-744-9773
508-745-3419
508-745-7942
508-746-8820
508-746-8256
508-746-8958
508-746-8674
508-747-2089
508-747-2068
508-747-2150
508-747-2854
508-761-8238
508-761-8382
508-761-8670
508-761-8801
508-761-8897
508-761-9790
508-822-1364
508-822-8835
508-822-8865
508-822-8902
508-822-8905
508-822-8906
508-823-2003
508-823-2007
508-823-2014
508-823-2070
508-823-2071
508-823-2076
508-823-6408
508-823-8002
508-823-8030
508-823-8079
508-823-9033
508-823-9710
508-824-1740
508-824-2949
508-824-3741
508-824-7362
508-824-9009
508-824-9013
508-824-9044
508-824-9061
508-824-9084
508-824-9092
508-824-9098
508-824-9109
508-824-9120
508-824-9125
508-824-9210
508-824-9213
508-824-9248
508-824-9271
508-824-9316
508-824-9321
508-824-9331
508-824-9342
508-824-9373
508-824-9382
508-824-9389
508-886-4838
508-880-0460
508-880-3739
508-880-3741
508-880-3780
508-880-6899
508-883-0172
508-883-0097
508-883-9440
508-883-9464
508-883-9477
508-883-9502
508-883-9512
508-883-9520
508-946-3493
508-946-5376
508-947-9763
508-947-9839
508-990-1406
508-990-2379
508-990-3877
508-990-9619
508-991-2330
508-991-2384
508-991-2473
508-991-4618
508-991-5026
508-992-2003
508-992-2184
508-992-8158
508-992-8353
508-992-8377
508-992-8472
508-992-8574
508-992-8853
508-995-3712
508-995-4109
508-995-8137
508-995-8309
508-995-8384
508-995-8860
508-996-1106
508-996-3083
508-996-3652
508-996-8126
508-996-8201
508-996-8227
508-996-8277
508-996-8325
508-996-8404
508-996-8577
508-997-3836
508-997-5251
508-998-2811
508-998-8601
617-242-9421
617-242-9422
617-242-9550
617-328-9603
617-472-9471
617-472-9473
617-695-3247
617-695-3357
617-695-8338
617-782-9366
617-787-5624
617-828-9615
617-828-8758
617-876-9826
617-871-3822
617-871-4573
617-871-5733
617-876-9469
617-876-9810
617-926-2102

Pages of Letters

Where One Hacker Went

Dear 2600:

The "Where Have All The Hackers Gone?" article in the Summer 1991 issue was relevant and personally powerful enough to bring me temporarily out of the "woodwork." I admit I am guilty of the article's charge of hackers "submitting to unacceptable terms and remaining underground like criminals."

Contrary to some of the rumors I have heard over the years, I was never arrested, never had my house searched, nor had anything confiscated. To me this seems like an absolute miracle due to the many security and law enforcement people who seemed intent on getting that "bastard, Lex Luthor." And no, I have never betrayed the trust of those who were then colleagues to avoid trouble with the law.

Perhaps my belief in freedom of speech and its consequent visibility, and not any alleged illegal acts perpetrated with a computer and modem, was what made me a target. *2600* has published my articles in many issues over the years. There were a number of other articles distributed electronically, which attempted to inform those who wanted to learn about the use and abuse of various technologies. And of course, my affiliation with the Legion of Doom helped to enlarge the bullseye.

I cannot say that my ego had nothing to do with writing "files," as being recognized for accomplishments, however dubious as they may have been, had some gratification. The drive to "fix the system" by informing people of the insecurity of computer systems was more of a factor in writing files than my ego was however. In retrospect, I realize that I was the one who needed the fixing and not the security.

For two and a half years I did not use a modem for any purpose, thus succumbing to the same fear that was mentioned in the article. Like Frank Darden, "I am a prisoner of my own hobby" with the obvious difference being that I am a free person. I will always live with the reality that my past transgressions may one day catch up with me. I never gained monetarily and I never acted with malice when I used my computer and modem. Yet I am still fearful. I suppose I am a victim of my own curiosity, the thrill of a challenge, and the enthusiasm of trying to inform others of what was out there. I was no "superhacker" nor "arch criminal."

Today I use computers sparingly. Like most people, my computer use is limited to assisting me with tasks that are too tedious to do "manually." And for the record, anytime I touch a computer it is for strictly legal purposes only. It appears to me that as one gets older one becomes more ethical. In my opinion, those who hold to the cliche "once a thief, always a thief" are obviously misguided, narrow minded, and distrusting of humanity as a whole including themselves. People can and do change.

The Atlanta hackers: Frank, Rob, and Adam have been sentenced to a life term of financial imprisonment. How can they pay the enormous fine levied against them plus their own legal fees, which I assume are astronomical, when most employers will not hire them in their field of expertise: computer science, due to their "background"? The punishment does not seem to fit the crime in this case.

It would be interesting to see a bulletin board that discussed hacking topics with some of the "old timers" who have gone underground along with the newly curious while remaining within the boundaries of the law. But with the current state of eroded civil rights and "shoot first, ask questions later" mentality, only the bravest of people would agree to run it.

I am relieved to see some respectable businesspeople taking a stand for everyone's rights, in the form of the Electronic Frontier Foundation (EFF). Victims like Craig Neidorf graphically depict the unjust state of affairs and the need to protect the Constitution. Perhaps the activities of the EFF and the current awareness of civil rights abuses is the reason I have finally acknowledged that I am indeed alive.

I am still a hacker in its pure sense: being curious, trying new approaches to problems, expanding the envelope, etc. The hacker in the darker sense is dead. Partly due to fear, partly due to necessity, partly due to self preservation, partly due to the realization that the ends do not justify the means.

As for where has this hacker gone, I have a four year engineering degree which took a bit more than four years partly due to all that time spent on computers which should have been spent studying. Today, I spend time hacking engineering design problems. Still fearful of persecution and prosecution, I am prevented from saying anything more. Perhaps I have said too much already.

(I used to be) Lex Luthor

Technical Questions

Dear 2600:

Why would I pay $4.50 an issue via subscription rather than the $4.00 newsstand price?

I'm not complaining, but your prices don't make sense. Look at the lifetime subscription price. $260 at four issues per year means that it won't begin to pay for 65 years. Also, why should a corporation pay more for a subscription than an individual?

I am glad to see your magazine out on mainstream newsstands. Hope you become as big as *Popcorn* and other hobby magazines.

MC
Austin, TX

We have what is known as a newsstand discount. If you get 2600 at a newsstand, it will cost slightly less than if you subscribe at the individual rate. We do this so more newcomers will get the magazine. Higher prices tend to discourage that kind of thing. The advantages to subscribing are convenience and timeliness: subscribers generally get their copies at least a week before any newsstands do. As to why corporations pay more than individuals, we find that large organizations require a substantial amount more attention than individuals. Purchase orders, invoices, billing notices, and phone calls are a normal part of the corporate world. We charge more to cover all of this and also because many corporations spread our articles to many different individuals. A special price for unlimited reproduction rights within an organization is actually not a bad deal. Regarding the lifetime subscriptions, it actually would begin to pay in just over 10 years, not 65. But that's not the point. Lifetime subscriptions are for those who want to and can afford to make a significant contribution to our continued operations. Were it not for those people who did this in the past, we would be in significantly worse shape than we are now. We are indebted to these kind souls for their generosity.

Raw Data

Dear 2600:

In parts of the 312 area code (Chicago), dialing 1-200-2356 returns a spoken voice reading the caller's phone number. For a quicker response, terminate with a #.

This is Illinois Bell's service for linemen. I got it by listening to the autodialer on Mr. Lineman's handset. I suppose if you print it, they'll change it, but what the hell.

The Militant Midget

By printing it, we also let people know it exists in the first place. If it isn't abused, there's no reason for it to be changed.

Dear 2600:

I thought I would share a few findings I have discovered about the tone dialer conversion to a red box. The red box works fine for long distance calls to other area codes or calls outside the immediate LATA I am calling from. However, I have found that when one places a long distance call to a nearby town that is served by the same Bell Operating Company (BOC) as the one I am calling *from*, the tones do not register well at all. You may have to beep in more money than is actually required before the ACTS computer is satisfied. Many people think this is because of the magnetic speaker inside the phone and the box itself. But if that were the case, then *all* calls, even those outside of the area code you are calling from would have problems with tones registering. I think the problem is that the local BOC equipment is more sensitive than the equipment used on long-haul AT&T long distance calls. Some suggest using a spacer about 1/2" thick over the phone receiver or holding the red box about 1/2" away from the receiver for accurate registration. This does not always work! A simple and easy cure to assure accurate registration of all red box tones is to force the call to be routed by AT&T and not the local BOC. Simply dial 10288 + 1 + the phone number you are calling. This forces the call to be handled by AT&T and the tones will register accurately. Remember, this is for calls to nearby towns that are served by the same BOC that you are calling from, but it doesn't hurt to use it all the time. Also, I have found that I do not have to insert one real nickel to red box with. This may not be cool in all areas of the USA, but it sure works in the South! I have talked for as much as 45 minutes without inserting any real coins, just using the beeps! As for a local call, I simply do not insert a quarter but dial "0" for operator. When she comes on, I tell her that I can't seem to dial the local number I wish to call. I ask her to dial it for me since the phone seems to be malfunctioning. She then dials it and tells me to insert the quarter. I then simply beep it in!

Also, I thought I'd tell you about a cheap-ass COCOT company called Coin-Call operating in Louisiana. They have their COCOTs placed at Kroger stores and other locations throughout Louisiana. As you know, the 214 area code split up into 903. Whenever you try to place a *legitimate* call to anywhere in the 903 area code from these COCOTs, the damn phones do not take the call! I assume these bastards think you are trying to dial a 1-900 call. I am not talking about trying to phreak the COCOT. You cannot dial a legitimate call to 903 no matter how you wish to pay! A good technique to use on these type of money-hungry corporations is to simply destroy the phone in my opinion. Super glue the lock and coin slot to prevent any further revenue being made by the company. Cut the receiver off the phone if possible or cut the phone line coming into the COCOT. I recently talked to a COCOT owner and he said his phones were extremely sensitive to lightning and electrical storms. He said anytime there was a storm in the nearby area, he had to check his COCOTs to be sure the rate chart was not reset to zero! If one could pierce the speaker of the phone with a sharp nail and then connect a device such as an electronic spark lighter like those used for starting barbecue fires, one could probably screw up the rate chart. Save your coins and call for free!

Arkansas Coin Collector

The only reason those COCOTs are not dialing into the 903 area code is because it hasn't been programmed into them yet. If you believe destroying the COCOT is the solution to this problem, we'd like to know what you have planned for the next AT&T outage. Perhaps leveling the state of New Jersey? While these kinds of "solutions" may make you feel better, they really don't do much to solve the problem. COCOT owners need to be held accountable, just like the phone companies. But many of us need to also be aware of the problems COCOT owners are faced with *because of unfair practices by the phone companies. COCOTs don't have access to the same technology that "regular" payphones do. Therefore, all of the technology must be built into the phone itself. If the system was really fair, the billing and routing information would not be controlled by a company that also operated payphones. Obviously their phones will get preferential treatment and the others will suffer. It's in the interest of the phone companies to make COCOTs as unappealing as possible. Think about this the next time you blow one up.*

Dear 2600:

As most of us know, the 800-933-3258 ANI demo line (Access Logic Technologies, Fort Worth, TX) is still in service, but only with a prior request (voice) call to the sales office (817-877-5629) to inform them that your "potential ANI customer" would like a line demo of their ANI system software, and their office will contact MCI, who will in turn allow ANI access for a designated period (usually three hours at a time). Probably not without MCI Security logging the call/request. Thus, there may be some apprehension to this method.

A tidbit of info on Access Logic Technologies: the president (Joe Sigler) is *also* Vice-Chairman of the Board for the Tandy Corporation. Now that is a very interesting item.

There is yet another procedure for ANI. Emergency 24, a nationwide alarm monitoring service in Chicago, has two 800 access lines: 800-282-0911 weekdays and 800-447-6168 weekends. Upon connection, a live operator will repeat back the number you are dialing from, through 800 ANI. To alleviate suspicion, you may then ask to be routed to "sales department voice mail," and your call will be truncated at that point. I'm sure the call is logged somewhere with AT&T. The ANI works regardless of whether the call is direct dial or operator assisted. Those two 800 numbers are AT&T provided, and the ANI information is processed despite the routing procedure. Placing the call through alternative carriers delivers the same end result.

Bellcore has a new publications listing of "tech inpho." "The Catalog of Technical Information" is a must for one's bookshelf. A call to 800-521-2673 has been established for a copy of their listing and for orders. Teltone Corporation of Bothell, WA has a "Telecom Design Solutions Catalog" for free with a call to 800-426-3926. Some interesting "application notes" can be found at the end of this rather thick supply catalog.

Finally, a couple of queries. Any readers know of any methods out there to block the ANI information on 800 calls? The service is available to all 800 subscribers, either with internal call-tracking and reporting formats right down to operator-station access. For those areas where ANI services are not yet available, it seems feasible that you could become an 800-service subscriber, have the CO remote-forward the call to your own number, and with ANI-800 ID hardware and software, voila, ANI! Do any readers know if it will actually work in application theory?

GS
Seattle

FAXers Beware

Dear 2600:

I just recently received my first issue of *2600* and I enjoyed it very much. However I was dismayed to see the box on page 45 about faxing a message. Fax transmissions are no safer than regular voice, or for that matter, data transmissions. There is an entire industry of facsimile monitoring and logging devices. One device, known as the STG Remote Satellite Logging System, is meant for law enforcement only, but the company will sell it for export. According to its description, "The Satellite Logging System is designed for acquiring facsimile transmission signals from telephone systems and converting these signals to a digital format. It then stores them onto a specially formatted DAT tape. The stored data can then be printed out at a central location for auditing with any of the other FAX MANager products. It is fully portable and housed in a rugged Halburton zero case. The unit is self powered by a built in rechargeable battery, or supplied by an AC adapter. The unit utilizes two working modes, 'auto' and 'manual.' The auto mode is used for the unattended recording of the facsimile signal. The manual mode is used for the playback of the signal, which can even be activated over the telephone line from a remote location to a central location where a STG FAX MANager is present."

SC
Hollywood, FL

And, from what we hear, they're virtually impossible to detect.

Prodigy Far From Gifted

Dear 2600:

I'd agree that Prodigy is a real turkey, if only for its on-screen advertisements, censorship of users' mail, and remarkably slow response. (Oh yeah, and its demands for a loaded PC or Mac that few home users can afford.) But STAGE.DAT really is the last straw.

Contrary to the bullshit given out by them when caught, it is clear that IBM and Sears did intend to read home computers.

I'm aware of two horror stories, first-hand in my role as a computer and private phone system technician, that prove this trick was done for and actually used for marketing purposes.

ONE: The STAGE.DAT file of one user was found to contain a whole group of mail addresses and telephone numbers when examined. Some of these did correspond to names and numbers in other modem programs the person used, and since these were in the same sub-directory path as Prodigy, there was a possible legitimate explanation.

The source of other names and numbers was a mystery as they didn't correspond to names and numbers in any modem dialing list. The user soon found that they were in word processing files, that is to say, in individually addressed letters. (The version of Wordstar used didn't have a telecom module.) Prodigy had read word processing files in a different subdirectory!

As a test, to rule out an accidental reading of files that were once physically stored where Prodigy is now, Wordstar was booted and a letter written to a dummy name with a phone number. Then Prodigy was contacted. After this, STAGE.DAT was looked at again. The new name and number was found within it. This proves that Prodigy deliberately incorporates this information every time it's run!

TWO: In a place where I do wiring work, LANs are used within departments to link PC's. If contact has to be made with another work group (whose LAN isn't gatewayed), it is done through modems, dialing through Centrex.

Now, due to the software involved, these other locations are given proper mailing addresses, numbers, and, since the software demands names, dummy names consisting of a name of the location as family and alpha mnemonics as given names are created. To wit: names like ABLE LEGAL, BAKER LEGAL, CHARLEY LEGAL, DELTA LEGAL, ABLE SALES, BAKER SALES, CHARLEY SALES, DELTA SALES, ABLE SHIPPNG, etc. are given to each computer.

Furthermore, these arbitrary computer "names" are never used outside the company. Also, in the company, a person sending a document to a certain computer in the legal department would know that it was in the legal department, but would never know the arbitrary first name given to that computer.

In short, there is no way, apart from reading the program, to know what arbitrary first names were given for system maintenance. And only management can read this password protected file.

Yet, shortly after installing Prodigy on several computers, junk mail from Prodigy arrived at the company addressed to such "people" as "ABLE SHIPPNG," "ABLE LEGAL," etc. showing that these names are captured and actually used for marketing purposes!

While MS-DOS has a well-known flaw that allows data to exist after it's been deleted, these two horror stories prove that it isn't an accident. It really was a deliberate process. They just got caught.

Big Al
Brooklyn

A most interesting account. We think you should demand an explanation from the Prodigy people. If the company can show that this information was not released in any way and can come up with the proof that such letters were received, it should get some attention. We've always found it disturbing that so many were so quick to excuse what was happening here without doing a thorough investigation. We hope more people continue to look into this and all future services that may do even worse things.

General Questions

Dear 2600:

I enjoy reading your fine, informative magazine (although I have never tried any of the interesting techniques described). There are a number of topics that I would like to have more information on and I was hoping that perhaps you might be able to help. These areas include:

A. Tempest. How does it work? Is it a real threat? How can we shield our equipment? How can we use this technology to observe others?

B. Since direct dialing is restricted by the U.S. to many overseas countries, is there a way to bypass this problem? Is it possible to, for example, dial to a number in Canada where no one is home and, while the phone is ringing, use the 2600 hertz tone to then get into the operator mode and enter the desired area code and number of the non-direct link country? Personally, I would be too afraid to even try such a technique.

C. When you receive a busy signal after dialing a number, I have heard that it is possible to listen to the conversation by first dialing a code and then redialing the number. Is this, or some variation of this, true?

D. Currently, New York State does not allow the phone company to offer ANI (Automatic Number Identification). Even though the state does not allow this, is it possible to determine the source of the incoming call prior to picking up the receiver or perhaps after the conversation, either by typing in a code or deciphering what is sent with the ring signal? Also, is it possible to protect the security of your phone number when you are making a call, by perhaps entering some type of code?

E. Two years ago, I received a telephone call from a senator. About ten minutes after our conversation, my phone started to do very strange things. The phone rang with a very low ringer sound nonstop for about fifteen seconds. When I picked up the phone, no one was there. This happened several times over the course of the next half hour. Can you explain what was happening?

Wilson Longline
New York

A. What you're referring to are surveillance receivers that can read what is on a CRT screen at distances of up to a couple of miles. One such device is the TSR 2000 made by Shield Research in Stockholm, Sweden (+46 8 6796205). Tempest equipment is shielded against this kind of thing. Short of expensive shielding, there are no real protections against this sort of thing. You can take comfort in the fact that within the next decade we'll probably be using more liquid crystal display (LCD) terminals and less CRTs. To the best of our knowledge, nobody can spy on these using radio waves.

B. That kind of trick has been used for quite some *time. It doesn't work as frequently anymore. But there's no reason why calls cannot be transferred legitimately in other countries to go to different places. For instance, calls to Albania could be placed through Canada before they were allowed from the United States. Canadians needing 800 numbers in the U.S. can't dial them directly. But it would be a great service if they could call a number in the U.S. which would then transfer them to the 800 number they wanted. Such a service wouldn't even cost the provider anything!*

C. Absolutely not.

D. What New York doesn't offer is Caller ID. ANI, however, is passed along to 800 numbers within the state just like anywhere else. Anyone with an 800 number can get the number of the people calling them in the majority of cases. One way to prevent your number from getting through is to go through an operator but we don't expect this method to last for long. In a way it's ironic that so much attention is being paid to the Caller ID issue when ANI just slipped in without any questions being raised. And, as far as most people are concerned, they're both doing the same thing. In answer to your question, it is not likely that the Caller ID signal is being sent out since the service is not being offered. For that reason, you needn't be concerned at this point about your number being sent out through Caller ID. But you're as vulnerable to ANI as anyone else.

E. For all we know, this happens every time a senator calls. We'll just have to ask around.

Red Box News

Dear 2600:

Here's a Radio Shack autodialer update. Make sure the metal can of the new crystal is not under any physical compression or stress when the autodialer is reassembled. In my initial conversion it resulted in intermittent operation (i.e., breakups in the series of tones). The unit should snap together without resistance or any bulges. I've noticed the autodialers use slightly different (but electronically equivalent) sized components and sometimes it's difficult to get the new crystal to fit just right without binding when putting the two halves back together during the conversion. On one unit I ended up removing the nickel-sized transducer near the speaker (it produces the high pitched beeps when in the programming mode) and mounting the crystal with a small square of double-faced tape to the circuit board area where the transducer is just above. It's a good comfortable placement if you can live without the programming beeps.

Also, in my area code (215), cellular telephones (serviced by GTE Mobilnet) can't call the 900 area code. Could it be because they don't send out Caller ID information? I had a friend with a cellular car phone call me on my Sprint 800 line. I carefully marked down the date and time of the call. When I received my phone bill and call detailing report, the cellular call wasn't on there. Can you explain this?

I tried the experiment a while later letting the phone ring five or six times before answering. This time my call detailing showed the number 360-0032 and listed the city as Pepper Pike, OH (a Cleveland suburb). This was a completely different number from my friend's cellular phone. When you call this number a recording repeats the number and says "it is being checked for trouble." I've heard this recording for weeks now. It's interesting I got a phone number at all on the 800 bill. Can you figure out what the story is here?

Pete in Akron

In all likelihood, the number is owned by GTE Mobilnet which uses it to place outgoing calls only. (Cellular phone numbers are not "real" like home phone numbers. ANI will not pick them up.) This explains why you get a recording when you try dialing in. The "being checked for trouble" recording could mean literally anything. We've seen them stay up for years.

Suggestions/Questions

Dear 2600:

I would consider myself a mid-level hacker, now post-adolescence. I remember the "old days" well, especially when manuals of *any* sort were impossible to obtain. I remember the good ol' days of RipCo (best in the Midwest), and miss it terribly. I have a little experience hacking into Milnet (from an Internet dialup, or local dialup to Milnet), more experience messing with Internet (about 2-3 years hard hacking), and various UNIX systems.

I've been a subscriber to *TAP* for a while, and even though the newsletter is disjunctional (at best), it has the true flavor of an underground publication. Please treat them with a little more respect, they're really good kids. After reading your publication (on and off) for a number of years, I am disturbed by the administrative trend you seem to be taking. Please, hire more people, and get more personal.

RN
Lake Forest, IL

We agree about TAP. But where the hell are they?! We haven't seen an issue in months! Being administrative is something we're not often accused of. We'll have to have a committee look into it.

Dear 2600:

While reading some of your back issues, I noticed ads for 2600 t-shirts and 2600 Eucro-stickers. Are these still available? If so, how much? Also, do you know of any Internet/Usenet node that has copies of *PHUN* magazine that are available for anonymous ftp?

Midnight Caller

You can try eff.org for back issues of various electronic hacker magazines. If PHUN isn't there, it shouldn't be too difficult to track it down. We'll have a new t-shirt out soon and, if we can get it together, other things. We'd like to hear ideas.

Dear 2600:

I'm writing in regards to a company mentioned in the Summer 91 issue, page 23 (International Micropower Corporation). I need a local phone number or address for this company because the 800 number listed in the article "The Class Struggle" does not work in Canada.

KS
Saskatoon, Sask.
Canada

The address we have for that company is 3355 West Spring Mountain Road, Suite 60, Las Vegas, NV 89102. We weren't able to get a local number for them.

Dear 2600:

In a recent issue, you provided an Atari virus. I was wondering if anyone associated with 2600 would have source code or infected disks of some of the recent MS-DOS "stealth viruses," in particular the Whale (alias: Mother Fish, Stealth Virus, Z The Whale) which was described in Patricia M. Hoffman's *Virus Information Summary List* (February 14, 1991 edition). As you are no doubt aware, *PHUN* has provided useful study material: Tesla Coil's "Viruses: Assembly, Pascal, Basic, and Batch" featured R. Burger's assembly code virus (Issue #3, Vol. 2, Phile 2) and Southern Cross presented the "Alameda College" Boot Infector Virus (Issue #4, Vol. 2, Phile 3). These viruses, however, are about five years old and some of the newer stealth viruses have more sophisticated anti-detection capabilities (in fact, many of them have no "destructive" dimension, they simply attempt to avoid detection and reproduce). Although I am a novice at programming, I find worms and viruses are a useful means of tackling "artificial life" questions because of their relative autonomy, reproductive ability, and interaction with their environment (particular platforms and operating systems). It is somewhat surprising that in Dr. Dobb's April 1991 special issue on Biocomputing, there was no mention of worms and viruses -- only such "legitimate" programs as neural nets, genetic algorithms, and fractals. If you can provide me with further information or point me in the right direction I would appreciate it.

GS
Ottawa, Ontario

We suggest looking in the 2600 Marketplace on page 41. If such information is available, that's where it will wind up.

Dear 2600:

My understanding is that there is a way to use your cellular phone to hear other phone calls other than your own (for test purposes only of course). This is supposed to work by entering a code into the phone's keyboard and then you can hear other cellular channels. I would like to try this out on my Mitsubishi transportable phone. I would be interested in seeing an article on how this can be done.

SS

We suggest reading the article "Cellular Phone Hopping" in the March 1991 issue of Monitoring Times. If we get additional info on this kind of thing, we'll print it.

Caller ID Decoders

Dear 2600:

It is now possible to obtain free Caller ID decoders! Motorola Semiconductor, Inc. of Austin, TX has announced their new MC145447, a fully integrated, single-chip Caller ID decoder and ring detector. The semiconductor device can be interfaced with LCD or LED displays, or a personal computer. The company is giving away *free* MC145447 sample kits with technical data to "qualified" electronic design engineers. Even the call is free! (Be prepared to give your company name and application requirements.) Motorola can be reached at (800) 521-6274.

Bernie S.

Hacking UNIX Passwords

Dear 2600:

In the last letters column, your editor and another letter writer criticized the program called Uhacker, published in the Spring 1991 issue because it was too easy to detect by system administrators. You both stated that an alternative and safer means of decrypting passwords was to get a copy of the /etc/passwd file and decrypting it at home. I have problems with this.

First of all, Mr. RJ stated that you should get a copy of the crypt source code (or something that works like it) from your target system, compile it, and use that to decrypt passwords. First of all, crypt() is a system call, which means that it is built into the kernel. Therefore, there is no source code for it, unless you have the source code for the kernel itself, and anyone who says they have that is full of it. The only thing related to crypt() that can be found in any libraries or "include" files will be the C interface to the kernel's internal machine language routines, which is essentially worthless for achieving our desired goal here.

Secondly, the encryption of passwords is unique to each system, which can be proven by comparing the same encrypted password entry on two different /etc/passwd files. They will be different. There are two possible reasons for this: a) each version of UNIX uses its own proprietary encryption routine, or b) they all use the standard DES encryption algorithm, but they each use their own unique encryption seed. Either way, there is no way you can get at any of this information, since it is built into the kernel itself. Assuming the latter, even if you had the DES encryption source code, you wouldn't have the key, which could be any input sequence of random bytes, something which would be unhackable.

If I am wrong, please tell me because I would love nothing more than to be able to safely implement what you guys are suggesting at home. As I see it, the only way to decrypt passwords is to do it directly off of the native system, which is, of course, very risky. Since your opening article encourages the free exchange of information rather than withholding it from less elite users, please explain how you would go about decrypting passwords at home, since you believe that you can do it.

SJ
New Haven, CT

UNIX is a standard, meaning that it was designed to behave the same to the user and programmer no matter what computer it is being run on. We do realize that it does vary a great deal from version to version and vary somewhat depending upon the implementation, but the output of a procedure like crypt() should be the same given the same input parameters. The key to the behavior of crypt() is the input parameters which consist of two strings or arrays of bits. They are presented as strings so that we can remember and read them. The first parameter is the "password" as we all know it. The second one is the "salt," a string made up of two possibly random letters that is used as the seed to generate the encrypted password. Fortunately for the password hacker program, the encrypted password starts with the same two letters as the salt, which gives us one of the two parameters to the crypt() procedure. This allows the brute-force approach of the program to guess the password even though the encrypted entry in the password file for a specific password might be different on a different system. If you create a new password twice, you are unlikely to obtain the same resulting encrypted password, because the "passwd" program usually relies on some randomness to generate the "salt" like the system clock.

Finally, you should be able to implement the crypt() routine at home, since the encryption algorithm is widely available.

Voice Mail Fun

Dear 2600:

I have discovered a major flaw in a voice mail system. It seems that ROLM PABX systems transfer all VMS messages to a centralized voice message bank. I have managed to find the voice bank number for British Petroleum (BP America). These numbers are toll free as an added extra.

The VMS requires an eight-digit username and up to (I believe) a 24-character password. Hence it's pretty hard to crack in large quantities. However, on calling the voice bank and entering the extension (of the person whose box you wish to open), the box opens. No username, no password, no protection. You can delete, save, listen to, transfer, and reply to messages for everybody in the company.

Nick
Newcastle Upon Tyne
England

We can assure you this doesn't work on any of the ROLM Phonemail systems we know. But it goes to show that bugs and deficiencies can always pop up.

There are many ways to send us letters. Our fax machine can be reached at 516-751-2608. Our Internet address is 2600@well.sf.ca.us. And for those of you who prefer the U.S. mail, our address is:

2600 Letters
PO Box 99
Middle Island, NY 11953

Letters may be edited for brevity or perhaps not printed at all! Anything is possible.

tidbits

You would think after all of the commotion about privacy invasion and lack of security that big corporations would begin to learn something. MCI can therefore be defined as learning-disabled.

You may have seen the ads for their Friends and Family Circle gimmick. Basically, you get your friends and family to sign up for MCI. Then, whenever you call them (assuming you too have MCI), you can save on the regular rates. In a way, MCI has gotten their customers to do their selling for them. That part is actually rather clever. In fact, we've even heard of families putting the guilt trip on relatives who refuse to sign up with MCI.

But where MCI really messed up is with their 800 FRIENDS update service. This number exists so that customers can check the status of their calling circle — find out who's currently on it, who's been dropped, etc. The touch tone service would ask you to key in your telephone number and then, to verify that it was really you, your zip code! Obviously, when you know somebody's phone number, figuring out their zip code isn't all that difficult. Yet this was the only bit of security standing in the way of *anyone* having access to customers' frequently dialed numbers. It made no difference if these numbers were unlisted. If they showed up on your calling circle, anybody could get them. And, not only that, but the relationship of the people in your circle was also announced. Example: "Your wife at 516-751-2600, your brother-in-law at 202-456-1414" and so on. One could get quite a bit of information on MCI customers rather quickly.

We had a bit of fun with this on WBAI's *Off The Hook*, the weekly telecommunications radio program in New York. We demonstrated the absurd security live on the air and told everybody to call MCI to complain. Apparently they did because the system was quickly changed. Now you need the last three digits of your account number for verification.

***

Those of you still mourning the loss of the various 800 ANI numbers can take comfort in a brand new number that's making the rounds. It's not an 800 number but we're told it doesn't charge. However the number won't work from payphones. It's 10732-404-988-9664. (You might have to dial a 1 before the 404.) It will only work with the 10732 carrier access code which is owned by AT&T. And for some reason, the recording seems to always add the number eight to the end.

***

It had to happen eventually. We finally found a 900 number that isn't a bad deal. For $1.50, you can call 900-884-1212 and get a reverse listing on a phone number, assuming it's listed. Telename of Springfield, VA has a database of over 80 million numbers and the human operators that answer don't try to keep you on for a long time. (If you do stay on, the cost is 75 cents a minute.) The only disadvantages are that numbers are only as updated as the most recent phone book from that region and the service is only staffed from 8 am to 6 pm, Eastern time, Monday through Friday. However, we hear that they will be automated before long.

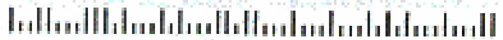
USPS HACKING

by The Devil's Advocate

The United States Post Office (USPS) is just like any other system. It is huge and complicated, with lots of acronyms and technical jargon. It is riddled with inconsistencies, and is prone to human error. Most importantly, it beckons to be explored by that very same bunch who are so fond of creative exploration: Hackers!

POSTNET

The Postal Numeric Encoding Technique (POSTNET) is a bar code system initiated in 1983 to help accelerate the sorting of letter mail by automated equipment. The term "POSTNET" refers to a bar code which represents either a five digit ZIP code, or a nine digit ZIP + 4 code. POSTNET is most often preprinted on business or courtesy reply mail by businesses. POSTNET can also be jet sprayed on envelopes that are processed by an Optical Character Reader (OCR) machine.



This POSTNET encodes 11953-0752.

POSTNET consists of a combination of 22 long bars and 30 short bars. The 52 bars encode a nine digit ZIP + 4 code plus a checksum number. Learning to read POSTNET is easy for anyone familiar with binary. The first and last bars (always long) are guide bars, and play no part in determining the encoded ZIP + 4. Each group of five bars after the first guide bar represents one ZIP + 4 number. The group consists of a combination of two long bars and three short bars. The position in the group has a corresponding value. The values from left to right are 7-4-2-1-0. A ZIP + 4 number is obtained by adding the values of the positions containing the two long bars. The only special case is when the added values equal eleven. In this case, the number represented is zero. POSTNET also includes a checksum number at the end for the purpose of error detection. You can determine what the checksum number should be by adding the numbers of your ZIP + 4. The last digit of the resulting sum, when subtracted from 10, will yield the checksum number. For instance, if your ZIP + 4 is 11953-0752, then the sum is 1+1+9+5+3+0+7+5+2=33, the last digit of the sum is 3, and the checksum is 10-3=7.

The USPS encourages companies to preprint the ZIP + 4 POSTNET on business reply mail by offering reduced postage rates. The advantage of using POSTNET is not only in savings but in speed. Letter mail that uses POSTNET is processed faster and more accurately than mail which does not use POSTNET.

MARK

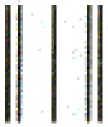
The MARK facer-canceler serves three purposes: 1) It cancels and postmarks letter mail; 2) It arranges letters so that they all face in the same direction; 3) It separates POSTNET letter mail from mail that does not use POSTNET.

The MARK utilizes fluorescent and phosphorescent detectors that enable it to detect the presence of minute traces of phosphor on stamps, pre-stamped postcards or envelopes, and meter marks. The MARK is also capable of detecting preprinted Facing Identification Marks (FIM).

FIM

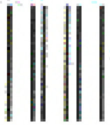
Open any magazine and you will find business reply mail cards inside. Nearly every card will contain a FIM. These six-line bar codes are much taller than POSTNET, but not nearly as wide. They are located at the top of the card, just left of the postage area. The MARK recognizes four types of FIMs:

FIM A



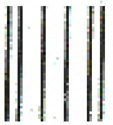
Letter uses POSTNET, and needs postage. Used for courtesy reply mail.

FIM B



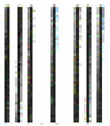
Letter does not use POSTNET, and does not need postage. Used for business reply mail.

FIM C

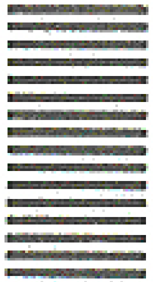


Letter uses POSTNET, and does not need postage. Used for business reply mail.

FIM D



Letter does not use POSTNET, needs postage, and is OCR readable. Used for courtesy reply window envelopes.



Business reply mail that uses FIM B or FIM C (indicating that no postage is necessary) must also use these horizontal bars to indicate that USPS must collect postage from the business to which the mail is addressed. The horizontal bars are located on the right hand side of the cards, and allow clerks to easily spot these cards in a tray full of other letters.

The MARK first checks to see that a letter has postage (stamp, meter mark, or FIM). After passing this test, the letter is then cancelled, postmarked, and directed to one of eight bins based upon the orientation of the letter and the presence of POSTNET. Four of the eight bins are for POSTNET letter mail, while the other four bins are for mail that does not use POSTNET. Each group of four bins accepts letters according to their orientation. Because letters can enter the machine right side up, upside down, backwards, or forwards, the MARK must have a bin for every possible orientation.

The MARK also utilizes a ninth bin for letters that are rejected by the machine for lack of postage. For example, if a letter does not have postage, and the letter does not have FIM B or FIM C (indicating that no postage is necessary), then the letter will end up in the reject bin. Sometimes letters that do have legitimate postage may end up in the reject bin. If a stamp is not placed in the upper right hand corner of an envelope, then the MARK's sensors may not detect the phosphor, and the letter will be rejected. A clerk manually goes over all of the rejected letters individually to determine why they were not processed.

LSM

The Letter Sorting Machine (LSM) was first used by the USPS in the late 1950's. The huge semiautomatic beast requires a group of operators to sit in front of twelve consoles while letters are zipping by at a rate of one per second. The machine automatically positions a letter in front of an operator, who then has one second to key in the first three digits of the ZIP code. The letter is then whisked away to one of several hundred bins according to the keys that were depressed. If an operator fails to key in anything then the letter will go to a reject bin and will eventually be fed back into the LSM. If an operator happens to key in the wrong code, then a slight possibility exists that the misguided letter will be caught by a clerk before it is shipped. Otherwise, the letter will be delivered to that location, wherever it may be, and will eventually be delivered back again.

LSM places a marker on the back of every letter that is processed. The marker consists of two alphanumeric symbols. The first symbol is always a letter ranging from A to Z. The second symbol is either a letter ranging from A to C, or a number ranging from 1 to 9. The marker can therefore be one of 319 possibilities. The marker may also be one of several different colors, although the color does not indicate any useful information. According to USPS LSM operators, the marker indicates which console processed the letter. However, this information is fairly useless because we still do not know which specific LSM processed the letter. The USPS uses hundreds of LSMs nationwide, and each of those LSMs has twelve consoles. I am uncertain how to translate a specific marker into a specific console, nor do I understand why the marker can be one of 319 possibilities if there are only twelve consoles.

BCS

The Bar Code Sorter (BCS) processes POSTNET letter mail. The BCS is therefore limited to sorting only business reply mail and other high volume mail which incorporates the POSTNET. At a sorting rate of ten letters per second, the BCS is considered slightly faster than your average clerk. The letters must be properly positioned and fed into the machine manually by an operator. This is accomplished by stacking trays of letters received from the MARK onto a feeder unit. The operator does not have to properly position each letter because the letters received from the MARK are already facing the same way.

MLOCR

The Multiline Optical Character Reader (MLOCR) is the latest and most advanced machine in the USPS letter sorting arsenal. This million-dollar monster is capable of reading all of the lines that comprise a letter's address. It then takes this information and compares it against its own internally stored address directory. Finally, an appropriate POSTNET is jet sprayed on the letter so that it can be further processed by a BCS. The purpose of the MLOCR is therefore to spray POSTNET on letters that do not use POSTNET, so that they can be processed by a BCS.

The advantage of the MLOCR is that it can determine an address even if parts of the address are illegible, incorrect, or missing. For instance, if someone forgets to include a ZIP code, or uses the wrong ZIP code by mistake, then the MLOCR can still determine the correct ZIP code by comparing the street, city, and state with its own address directory. It will then spray the letter with the correct ZIP + 4 code (the MLOCR will always try to spray the letter with a ZIP + 4, even if the letter uses a five digit ZIP code).

Early OCRs could only read type or clearly printed handwriting. In the near future, however, the MLOCR will recognize script as well. The MLOCR is capable of reading the address even if it is skewed (i.e. printed at an angle). The MLOCR does not have the capability of knowing whether or not a letter already has POSTNET, nor can it sort mail according to POSTNET. Therefore, it is possible to receive a letter that has two overlapping POSTNET bar codes.

Like the BCS, the MLOCR only accepts trays of properly positioned machinable letters that must be fed into the machine manually by an operator.

Mail Hacks

There are at least three things that everyone familiar with the USPS would like to do: 1) Mail letters for free; 2) Get their letters delivered quicker; 3) Find out why it takes so long for their letters to arrive.

Free Mail

It is not difficult for someone to mail a letter for free. It is, however, extremely difficult to mail many letters for free. The USPS is always looking out for mail fraud, and has an entire agency devoted to just this task. Even if a good mail hack works once, it is not likely to work if used repeatedly. Therefore, if you are reading this article with the intent of saving money by tricking the USPS and mailing letters for free, then you would do better to give up now before you are busted. Of course, anyone with even the slightest iota of curiosity would want to know some of the methods.

Perhaps one of the oldest scams in the book is to switch the destination address with the return address and mail the letter without postage. The USPS will then return the letter to its "sender" for postage. Of course, the USPS is not that stupid, and this trick rarely works for nonlocal mail.

A much better mail hack would be to use a laser printer to print a FIM B on an envelope. The MARK will then treat this letter like a business reply mail card, and will not reject it for lack of postage. Of course, the problem with this technique is that a mail carrier will almost certainly notice the missing postage before the letter even gets to a MARK. Therefore, you would have to bundle this letter with another letter that has postage, place the letter with postage on top of the illegitimate letter, and use a rubber band to bundle them together. The mail carrier will not disturb this bundle. Eventually, the bundle will reach a General Mail Facility (GMF) where clerks quickly separate bundles on a conveyor belt. It is extremely unlikely that they will notice the illegitimate letter at this point. From the conveyor belt, the letter will journey to the MARK. Once the MARK processes the letter, it is unlikely that anyone will notice the missing postage until the letter reaches its destination. The final obstacle is the mail carrier that will physically deliver the letter to its destination. At this point, the letter is postmarked, so one can only hope that the mail carrier is not too nosy.

Fast Mail

Getting your letters mailed quickly is a much better hack than trying to mail your letters for free. Not only is it legal but the results are guaranteed.

Normally, a letter reaches a MARK where it is processed and sent to an MLOCR. If the address on the envelope is readable by the MLOCR, then it is jet sprayed with a POSTNET and sent to a BCS. Otherwise, the letter is rejected and sent to an LSM. The one thing you really want to avoid is having your letter processed by an LSM. The operators who run these machines are notorious for keying in the wrong code, causing your letter to journey out of its way to strange and exotic parts of the country. Never write the address on your envelope in script unless you want to delay your letter.

One way you can get your letters processed quicker is to have your letters skip some of the steps in the sorting process. The method involves using a laser printer to print a FIM A and a POSTNET on an envelope. The FIM A will instruct the MARK to treat the envelope as courtesy reply mail. The MARK will look for postage, which you have thoughtfully provided, and then send the letter into a bin with all of the other POSTNET mail. This mail will then be placed in a tray and sent directly to a BCS, skipping the MLOCR and completely avoiding the LSM.

By using POSTNET, you are taking advantage of the same multimillion dollar equipment that is used by businesses.

Another advantage to using this method is that your letter will be processed entirely by machines. From the moment your letter enters the MARK until the moment it leaves the BSC, no clerk will see your letter. In addition, the USPS will be pleased with your creative use of their multimillion dollar machinery.

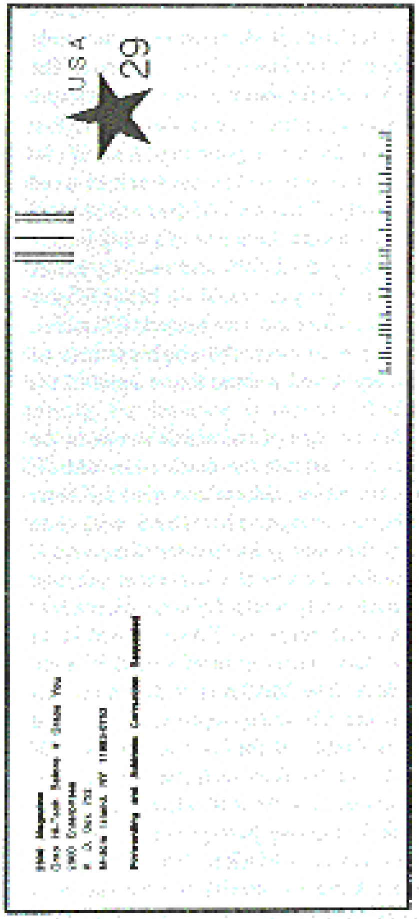
Snail Mail

Now that you know what happens to your letter when you mail it, you can use this information to determine why it takes so long for your own mail to arrive. The next time a letter comes in the mail, analyse it for telltale USPS markings that may give you insight into how the letter was processed. If the letter has POSTNET on it, then you know that the letter was processed by an MLOCR and a BCS. You can then read the POSTNET to make sure that it represents your ZIP code. If the POSTNET is incorrect then that would certainly explain why your letter was delayed. You should also flip the letter over and look for LSM markers. You should not see any more than one or two markings. If the back of your letter is covered with them, then you know that your letter probably had quite a journey whipping back and forth around the country before it reached you. Keep in mind that it is not unusual for a letter to be processed by both a BSC and an LSM. Not all GMFs use the same machinery, and the average clerk can screw up any letter, even if it is processed by machines.

Further Reading

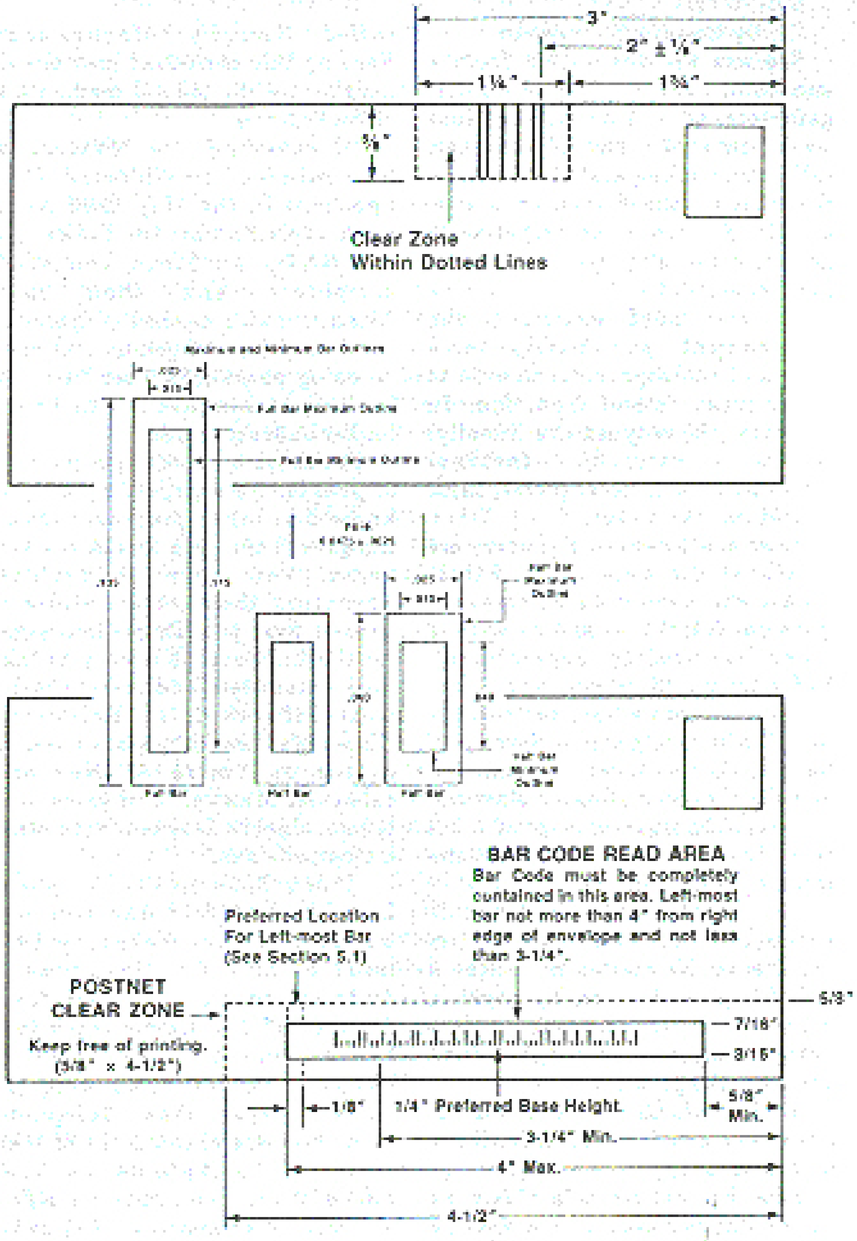
For those of you who are interested in learning more about POSTNET and the machines that process mail, we suggest that you obtain *A Guide to Business Mail Preparation*. The pamphlet is produced by the USPS (Publication 25) and is available free-of-charge to all business customers. You can request a copy through the mail by writing to this address:

Marketing Department
Regular Mail Services Division
U.S. Postal Services Headquarters
475 L'Enfant Plaza SW, Room 5541
Washington D.C., 20260-6336


USA
29
2600 Magazine
Grab Hi-Tech Before it Grabs You
2600 Enterprises
P. O. Box 752
Middle Island, NY 11953-0752
Forwarding and Address Correction Requested

We designed the FIM A and the POSTNET on this envelope using standard desktop publishing software. A laser printer was used to print the two barcodes on the prestamped envelope. If we ever decide to mail this letter, it should get back to us with all of the speed afforded to courtesy reply mail.

This information was obtained from ***A Guide to Business Mail Preparation*** (Publication 25). Use these diagrams to design your own FIM and POSTNET.



PSYCHOLOGY IN THE HACKER WORLD

by Condor Woodstein

We are all descended from a successful tribe of 15 to 30 hunter-gatherers, so it is no surprise that we fall into categories. Mythologists call them archetypes: the Orphan, the Warrior, the Wanderer, and so on. The Enforcer is an archetype, a genetic personality type that exists in every society.

At its most extreme, the enforcement personality is a paranoid schizophrenic, unable to distinguish friend from foe. In America, these types are (ideally) ferreted out by Internal Investigations. In other places, these crazies rule the nation.

First and foremost, Enforcers are convinced of the rightness of their ideas. Philosophical doubts are unheard of. If the legislature were to make hard-boiled eggs illegal, Enforcers would pursue people who sell and consume hard-boiled eggs with the same vigor now devoted to hackers. In this sense, the Enforcer actually shows an amazing elasticity of belief. The mere passage of a bill into law will re-organize the thinking of the Enforcer.

As a corollary, the Enforcer is incapable of learning from experience. No matter how often a belief is proved wrong by physical evidence, the Enforcer claims that better equipment or tougher laws will solve the problem.

William J. Cook is the federal prosecutor who busted Shadowhawk and who stopped the presses at *Phrack*. He told the tale of how he nailed Shadowhawk in a magazine called *Security Management*. Reading this periodical provides an insight into the mental mechanisms of the Enforcer.

"Uncovering the Mystery of Shadowhawk," by William J. Cook appeared in the May 1990 issue. Cook explains how the hacker got into NATO, Air Force, and AT&T computers and then says, "Shadowhawk's method of operation was based less on genius and more on using passwords, user tips, and hacking techniques learned from hacker bulletin boards."

The above is an example of *denial of genius*. As a programmer, you know that other programmers do things well that you do not and vice versa. You have no problem admitting that someone else is smarter than you. This is impossible for the Enforcer. It is easy to take Cook's statement and make it into a Nazi refutation of Relativity: "Einstein's theories are based less on genius and more on Newton's calculus, Maxwell's physics, and tensor algebra learned from other mathematicians."

"Doing Time on the Telephone Line," by Langford Andersen was published in the February 1990 issue of *Security Management*. Anderson is the communications director of The Communications Fraud Control Association in McLean, Virginia. In outlining the many ways that telephone companies are cheated out of their revenues, he explains the "code calling" fraud, perpetrated on AT&T by trucking companies. "The caller would ask the operator to place a collect call for Fred P. Jones III. The call would be refused, but the name was a code that let the company know a driver has half a load in Nashville en route to Kansas City. This would go on 24 hours a day, seven days a week, and the cost in AT&T operator time was incredible."

This is an example of denial of opportunity. AT&T defined its own system. Yet by taking advantage of that system, these trucking companies committed "fraud" in the eyes of the Enforcer.

It is also an example of *tunnel vision*. Trucking companies were not the only ones who benefited from this insight. Salesmen calling home, college kids, millions of people took advantage of this loophole in AT&T policies. The fact that AT&T survived suggests that these costs were already built into the phone rates. Perhaps we are to believe that this activity leapt into sudden existence in 1970 and only divestiture saved the company.

Yet another example of this *tunnel vision* comes from Brian D. Costley's "Cracking Down on the New Safecracker." No, it isn't a reincarnation of Richard P. Feynman, it's an autodialer that can spin 230,000 combinations in 30 hours. The article surrounds an ad for combination locks by Sargent and Greenleaf, the company that employs Costley. This blatant example of feathering one's own nest is lost on the Enforcer who passively accepts the offerings of any authority figure. Simple arithmetic would indicate that the S&G dual-dial combination locks are only a bigger, not impenetrable, barrier. It is almost humorous that the S&G ad relies on registered trademark phrases: "spy-proof" and "manipulation-proof." (Think of how cool it would be to nail a sign to your home that says "Windsor Castle (r).")

Despite the image of the Enforcer who is dedicated to facts (promulgated by police procedural mysteries), the truth is that at some point, the belief structures of the enforcer can only be protected by vagueness.

An example of this *denial of objective reality* can be found in "Defending Against Virus Attacks," by Raymond G. Kammer, the deputy director of the National Institute of Standards and Technology. The article appeared in the May 1990 issue of *Security Management*.

How does one defend against viruses? No answer is given. The article alludes to private sector solutions, but none is named. The article describes committees, studies, and news releases. In response to the Internet Worm (he calls it a "virus"), the NIST worked with the Department of Defense and the National Security Agency. Rather than create computer programs, they created another committee which in turn warned computerists about the Columbus Day Virus of 1989 but failed to provide any products.

For many Enforcers, this divorce from reality eventually manifests itself as *paranoia*. A perfect example of the denial mechanisms involved comes from "Headache for the Host" by Darlene M. Tester, *Security Management*, January 1990. The article is a complaint against "a new protocol in data processing — file transfer from PC to host." The author also says, "A thorn in the side of the software industry has been public domain software.... In the past, these software packages have been available through PC network bulletin boards and pirate data reproduction services.... File transfer protocols are entering this sector of the software industry.... Unlike other public domain packages, this software comes under the guise of a different name — 'nonpublic domain' software."

Tester's solutions to the threat of file transfer protocols are to forbid users from mounting such software. Failing that, if users are actually permitted to load programs, then the system administrator must "print a hardcopy of the protocol and review it for logic bombs or time bombs." If she can read hex code that well, I admit she is smarter than I'll ever be.

Projection and transference are psychological mechanisms that manifest themselves strongly in neurotic individuals. Tester uses the phrase "fairy tale existence" and accuses unnamed persons of claiming that unnamed security people are "paranoid."

Continuing not to name names, Tester alludes to "name-brand protocol systems" that are safe and reliable, but doesn't name any. Tester closes her article with the paranoiac's manifesto: "Host systems have a good safety record. That safety record must be maintained at all costs." Would Tester draw the line at executing one Eskimo in ten if it meant that mainframes would be safe from viruses? You can gauge the level of *reality denial* by considering that, as a woman, Tester is a "host." She fears "mounting," "penetration," and "infection" and in fact, "has a headache." If she would face these fears, they wouldn't appear in her technical essays.

You can see from these examples that the Enforcer is a terrible servant and a fearful master. Only the strongest judicial and constitutional restraints will protect America from these deluded individuals.

2600 has meetings in New York and San Francisco on the first Friday of every month from 5 pm to 8 pm local time. See page 41 for specific details.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

WANTED: Schematics and data kits for telephone line voice scramblers. Prefer digital units using DES encrypt/decrypt algorithm. Code key must be user changeable from exterior of unit. Please send price/details to A.G. Morris, PO Box 4682, Long Beach, CA 90804-4682.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people tracers - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Shoreham, NY 11786. FAX 516-929-0772.

WILL PAY $10,000 for "mind radio" computer program and schematics. Call Mike at 212-533-4351.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. **$10 off** for 2600 subscribers. Surveillance Countersurveillance equipment catalog $5. Miniature Surveillance Transmitter Kits $39.95 ppd. Voice changers, scramblers, vehicle tracking, bug and phone tap detectors, books, videos, etc. E.D.E., PO Box 337, Buffalo, NY 14226 (716) 691-3476.

CAN SUPPLY software and computer hardware of any kind below wholesale prices. I am looking for sales people. If you can find me buyers, I will work out a percentage. Would like to correspond with hackers in Switzerland, Germany, Japan, and France. Anybody with access to stealth bomber technology or access to Los Alamos National Laboratory in New Mexico and/or Lawrence Livermore Labs in San Francisco. K. Henderson, PO Box 265, Agoura Hills, CA 91301. 818-889-8351.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs, soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it. (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

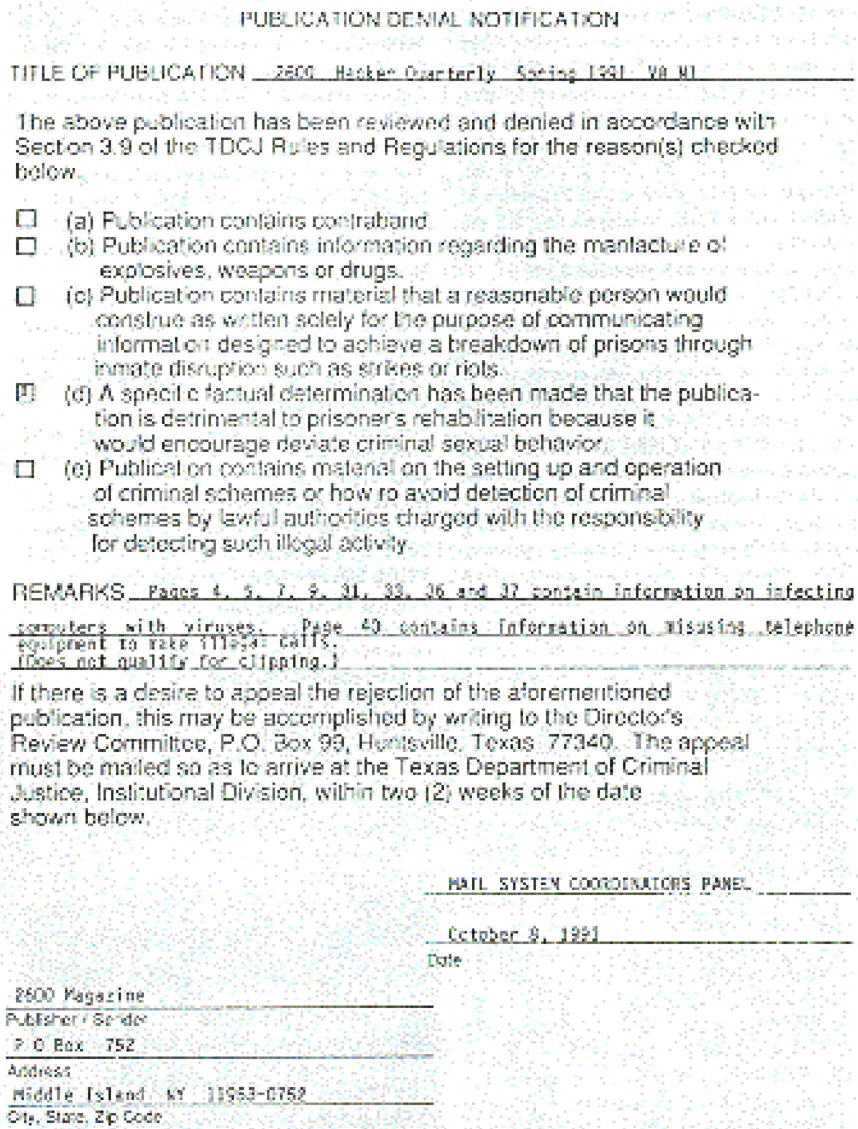
COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 1/15/92.

MORE EXCITING PRISON NEWS



PUBLICATION DENIAL NOTIFICATION

TITLE OF PUBLICATION 2600 Hacker Quarterly Spring 1991 V8 N1

The above publication has been reviewed and denied in accordance with Section 3.9 of the TDCJ Rules and Regulations for the reason(s) checked below.

□ (a) Publication contains contraband.

□ (b) Publication contains information regarding the mantacture of explosives, weapons or drugs.

□ (c) Publication contains material that a reasonable person would construe as written solely for the purpose of communicating information designed to achieve a breakdown of prisons through inmate disruption such as strikes or riots.

☒ (d) A specific factual determination has been made that the publication is detrimental to prisoner's rehabilitation because it would encourage deviate criminal sexual behavior.

□ (e) Publication contains material on the setting up and operation of criminal schemes or how to avoid detection of criminal schemes by lawful authorities charged with the responsibility for detecting such illegal activity.

REMARKS Pages 4, 5, 7, 9, 31, 33, 36 and 37 contain information on infecting computers with viruses. Page 40 contains information on misusing telephone equipment to make illegal calls.
(Does not qualify for clipping.)

If there is a desire to appeal the rejection of the aforementioned publication, this may be accomplished by writing to the Director's Review Committee, P.O. Box 99, Huntsville, Texas 77340. The appeal must be mailed so as to arrive at the Texas Department of Criminal Justice, Institutional Division, within two (2) weeks of the date shown below.

MAIL SYSTEM COORDINATORS PANEL

October 9, 1991
Date

2600 Magazine
Publisher / Sender
P O Box 752
Address
Middle Island NY 11953-0752
City, State, Zip Code

Our magazine has been called just about everything under the sun, but this is a new one on us.

more conversion tricks

by DC

The Radio Shack red box conversion is the greatest example of a remarkable coincidence that I have ever come across. The fact that the timing of the microprocessor inside the device and the tone pair for the DTMF asterisk when sped up creates a nearly perfect quarter tone sequence is beyond luck. The entire conversion is poetry. Thanks for the great work, Noah Clayton.

Being that the tone dialer itself is such a nice product (I believe it is, feature for feature, the best product Radio Shack has to offer, considering most of what Radio Shack has to offer sucks and is overpriced anyway) I didn't want to just convert mine into a red box. I wanted to have the red box tones as well as the dialer capabilities. Since reading the conversion article in the Autumn 1990 issue of *2600*, I have come across a file explaining how to make the conversion but incorporating a switch to select between the two different frequency crystals, enabling both touch tones and a red box. One thing I didn't like about the file's design is that it had wires coming out of the back of the unit to the two crystals and the switch which were all epoxied together to the back of the unit. Ugly. I managed to fit everything neatly inside the unit.

The first thing I did was file the lip on the bottom of the 6.5536 Mhz crystal flush with the rest of its case to give it a lower profile. Looking at the circuit board with the battery compartment towards you, I removed the screw on the upper left-hand side near the two solder pads and diode and put the crystal in that area. I also reduced the solder on the lower pad to make the slightest bit more room for the crystal. I soldered one lead of the 6.5536 Mhz crystal (extended with a piece of wire) to one lead of the 3.579545 Mhz crystal. I then soldered the other lead to the top leg of the SPDT switch and glued the crystal in place with some super glue. I then desoldered the other leg of the 3.579545 Mhz crystal and jumpered it to the bottom leg of the SPDT switch. Finally, I soldered a jumper from the middle leg of the switch to the lead into the microprocessor (the lead that one leg of the 3.579545 Mhz crystal was desoldered from). I cut a slot in the side of the two halves of the case (the side opposite the ON/OFF and DIAL/STORE switches) and glued the switch in place. It works like a charm.

The 6.5536 Mhz crystal can also be ordered from Radio Shack, by the way, for $4.95 each. I wouldn't mention this if it weren't for the fact that Fry's Electronics wanted to charge me eight bucks shipping and handling alone on a cash order.

I also discovered that the tone dialer can be converted to generate the green box "coin return" tone. Replacing the 3.579545 Mhz crystal with one that has a value close to 4.1521 Mhz (the calculated value) will cause the pound (#) key to generate frequencies close enough to the 1100 and 1700 Hz green box tones (1091 and 1713 in actuality). Making this mod to the dialer wouldn't suffice because you would still need a way to generate either 2600 Hz or 900+1500 Hz (the "operator release" signal) in order to send the green box tones. If someone can figure out how to incorporate all needed green box tones into the dialer, I would like to hear about it. It would be a nice complement to the red box.

Readers. Please send us your experiences and experiments to share

useful unix programs

by Marshall Plann

THIS PROGRAM LETS YOU SEE WHAT ANY WORD WILL LOOK LIKE AFTER IT'S CRYPTED. THIS IS PARTICULARLY USEFUL FOR THE NEXT PROGRAM.

```
#include <pwd.h>

main(argc,argv)
int argc;
char *argv[];
{
   if (argc>2)
      printf("%s\n",crypt(argv[1],argv[2]));
   else if (argc>1)
      printf("%s\n",crypt(argv[1],"hi"));
}
```

THIS PROGRAM WILL ALLOW YOU TO LOCK UP ANY TERMINAL ON A UNIX SYSTEM UNTIL THE SECRET WORD IS ENTERED. IN THIS CASE, THE SECRET WORD IS DOG. THE WORD IS LISTED IN ENCRYPTED FORM, OTHERWISE ANYONE LISTING YOUR PROGRAM WOULD BE ABLE TO SEE IT.

```
/*
save this as "secret.c" and
type "make secret" or "cc secret.c -o secret"
to compile.
*/

#include <stdio.h>
#include <sys/ioctl.h>
#include <signal.h>
#include <pwd.h>

main(argc,argv)
int argc;
char **argv;
{
   struct  sgttyb  basic;
   short flags;
   char str[32];
   int i;

   /* ignore all interrupts that may try
     to mess up this program like ^C ^Z */
   for(i=1;i<33;signal(i++,SIG_IGN)) ;

   /* shut off echo and receive key strokes
     as they are hit from the terminal */
   ioctl(fileno(stdin), TIOCGETP, &basic);
   flags = basic.sg_flags;
   basic.sg_flags |= CBREAK;
   basic.sg_flags &= ~ECHO;
   ioctl(fileno(stdin), TIOCSETP, &basic);

   do {
      /* prompt for the input */
      fprintf(stdout,"Enter Secret Word>");
      fflush(stdout);

      /* get the input until a return
        or a lot of keys are hit */
      for(i = 0;(i<31)&&((str[i] = getchar()) !=
'\n');i++) ;

      /* terminate the string */
      str[i]= '\0';

      /*      acknowledge that you have
              accepted the return by echoing it
*/
      fprintf(stdout,"\n");

      /* repeat until the word
        has been entered */
   }
while(strcmp(crypt(str,"hi"),"higSfxQjrCp7Y"
));

   /* restore the terminal back to
     the original settings */
   basic.sg_flags = flags;
   ioctl(fileno(stdin), TIOCSETP, &basic);

   /*  do something with the secret string
      here, I just print it out...
      you could have fun with it
   fprintf(stdout,"->%s\n",str);
   fflush(stdout);
   */
}
```

```
2 (145)
3 (145)
1 (234)
5 (234)
1 (245)
4 (235)
1 (245)
3 (245)
1 (345)
2 (345)
(1234)
(1235)
(1245)
(1345)
(2345)
```

**GROUP D:
451**

```
1 2 3 4 5
1 2 3 5 4
1 2 4 5 3
1 2 4 3 5
1 2 5 3 4
1 2 5 4 3
1 3 4 5 2
1 3 4 2 5
1 3 5 2 4
1 3 5 4 2
1 3 2 4 5
1 3 2 5 4
1 4 5 2 3
1 4 5 3 2
1 4 2 3 5
1 4 2 5 3
1 4 3 5 2
1 4 3 2 5
1 5 2 3 4
1 5 2 4 3
1 5 3 4 2
1 5 3 2 4
1 5 4 2 3
1 5 4 3 2
2 1 3 4 5
2 1 3 5 4
2 1 4 5 3
2 1 4 3 5
2 1 5 3 4
2 1 5 4 3
2 3 4 5 1
2 3 4 1 5
2 3 5 1 4
2 3 5 4 1
2 3 1 4 5
2 3 1 5 4
2 4 5 1 3
2 4 5 3 1
2 4 1 3 5
2 4 1 5 3
2 4 3 5 1
2 4 3 1 5
2 5 1 3 4
2 5 1 4 3
2 5 3 4 1
2 5 3 1 4
2 5 4 1 3
2 5 4 3 1
3 1 2 4 5
3 1 2 5 4
3 1 4 5 2
3 1 4 2 5
3 1 5 2 4
3 1 5 4 2
3 2 4 5 1
3 2 4 1 5
3 2 5 1 4
3 2 5 4 1
3 2 1 4 5
3 2 1 5 4
3 4 5 1 2
3 4 5 2 1
3 4 1 2 5
3 4 1 5 2
3 4 2 5 1
3 4 2 1 5
3 5 1 2 4
3 5 1 4 2
3 5 2 4 1
3 5 2 1 4
3 5 4 1 2
3 5 4 2 1
4 1 2 3 5
4 1 2 5 3
4 1 3 5 2
4 1 3 2 5
4 1 5 2 3
4 1 5 3 2
4 2 3 1 5
4 2 3 5 1
4 2 5 1 3
4 2 5 3 1
4 2 1 3 5
4 2 1 5 3
4 3 5 1 2
4 3 5 2 1
4 3 1 2 5
4 3 1 5 2
4 3 2 1 5
4 3 2 5 1
4 5 1 2 3
4 5 1 3 2
4 5 2 1 3
4 5 2 3 1
4 5 3 1 2
4 5 3 2 1
5 1 2 3 4
5 1 2 4 3
5 1 3 2 4
5 1 3 4 2
5 1 4 2 3
5 1 4 3 2
5 2 3 1 4
5 2 3 4 1
5 2 4 1 3
5 2 4 3 1
5 2 1 3 4
5 2 1 4 3
5 3 4 1 2
5 3 4 2 1
5 3 1 2 4
5 3 1 4 2
5 3 2 1 4
5 3 2 4 1
5 4 1 2 3
5 4 1 3 2
5 4 2 1 3
5 4 2 3 1
5 4 3 1 2
5 4 3 2 1
(12) 3 4 5
(12) 3 5 4
(12) 4 3 5
(12) 4 5 3
(12) 5 3 4
(12) 5 4 3
(13) 2 4 5
(13) 2 5 4
(13) 4 2 5
(13) 4 5 2
(13) 5 2 4
(13) 5 4 2
(14) 2 3 5
(14) 2 5 3
(14) 3 2 5
(14) 3 5 2
(14) 5 2 3
(14) 5 3 2
(15) 2 3 4
(15) 2 4 3
(15) 3 2 4
(15) 3 4 2
(15) 4 2 3
(15) 4 3 2
(23) 1 4 5
(23) 1 5 4
(23) 4 1 5
(23) 4 5 1
(23) 5 1 4
(23) 5 4 1
(24) 1 3 5
(24) 1 5 3
(24) 3 1 5
(24) 3 5 1
(24) 5 1 3
(24) 5 3 1
(25) 1 3 4
(25) 1 4 3
(25) 3 1 4
(25) 3 4 1
(25) 4 1 3
(25) 4 3 1
(34) 1 2 5
(34) 1 5 2
(34) 2 1 5
(34) 2 5 1
(34) 5 1 2
(34) 5 2 1
(35) 1 2 4
(35) 1 4 2
(35) 2 1 4
(35) 2 4 1
(35) 4 1 2
(35) 4 2 1
(45) 1 2 3
(45) 1 3 2
(45) 2 1 3
(45) 2 3 1
(45) 3 1 2
(45) 3 2 1
3 (12) 4 5
3 (12) 5 4
4 (12) 3 5
4 (12) 5 3
5 (12) 3 4
5 (12) 4 3
2 (13) 4 5
2 (13) 5 4
4 (13) 2 5
4 (13) 5 2
5 (13) 2 4
5 (13) 4 2
2 (14) 3 5
2 (14) 5 3
3 (14) 2 5
3 (14) 5 2
5 (14) 2 3
5 (14) 3 2
2 (15) 3 4
2 (15) 4 3
3 (15) 2 4
3 (15) 4 2
4 (15) 2 3
4 (15) 3 2
1 (23) 4 5
1 (23) 5 4
4 (23) 1 5
4 (23) 5 1
5 (23) 1 4
5 (23) 4 1
1 (24) 3 5
1 (24) 5 3
3 (24) 1 5
3 (24) 5 1
5 (24) 1 3
5 (24) 3 1
1 (25) 3 4
1 (25) 4 3
3 (25) 1 4
3 (25) 4 1
4 (25) 1 3
4 (25) 3 1
1 (34) 2 5
1 (34) 5 2
2 (34) 1 5
2 (34) 5 1
5 (34) 1 2
5 (34) 2 1
1 (35) 2 4
1 (35) 4 2
2 (35) 1 4
2 (35) 4 1
4 (35) 1 2
4 (35) 2 1
1 (45) 2 3
1 (45) 3 2
2 (45) 1 3
2 (45) 3 1
3 (45) 1 2
3 (45) 2 1
3 4 (12) 5
3 5 (12) 4
4 3 (12) 5
4 5 (12) 3
5 3 (12) 4
5 4 (12) 3
2 4 (13) 5
2 5 (13) 4
4 2 (13) 5
4 5 (13) 2
5 2 (13) 4
5 4 (13) 2
2 3 (14) 5
2 5 (14) 3
3 2 (14) 5
3 5 (14) 2
5 2 (14) 3
5 3 (14) 2
2 3 (15) 4
2 4 (15) 3
3 2 (15) 4
3 4 (15) 2
4 2 (15) 3
```

```
4 3 (15) 2
1 4 (23) 5
1 5 (23) 4
4 1 (23) 5
4 5 (23) 1
5 1 (23) 4
5 4 (23) 1
1 3 (24) 5
1 5 (24) 3
3 1 (24) 5
3 5 (24) 1
5 1 (24) 3
5 3 (24) 1
1 3 (25) 4
1 4 (25) 3
3 1 (25) 4
3 4 (25) 1
4 1 (25) 3
4 3 (25) 1
1 2 (34) 5
1 5 (34) 2
2 1 (34) 5
2 5 (34) 1
5 1 (34) 2
5 2 (34) 1
1 2 (35) 4
1 4 (35) 2
2 1 (35) 4
2 4 (35) 1
4 1 (35) 2
4 2 (35) 1
1 3 (45) 2
1 2 (45) 3
2 1 (45) 3
2 3 (45) 1
3 1 (45) 2
3 2 (45) 1
3 4 5 (12)
3 5 4 (12)
4 3 5 (12)
4 5 3 (12)
5 3 4 (12)
5 4 3 (12)
2 4 5 (13)
2 5 4 (13)
4 2 5 (13)
4 5 2 (13)
5 2 4 (13)
5 4 2 (13)
2 3 5 (14)
2 5 3 (14)
3 2 5 (14)
3 5 2 (14)
5 2 3 (14)
5 3 2 (14)
2 3 4 (15)
2 4 3 (15)
3 2 4 (15)
3 4 2 (15)
4 2 3 (15)
4 3 2 (15)
1 4 5 (23)
1 5 4 (23)
4 1 5 (23)
4 5 1 (23)
5 1 4 (23)
5 4 1 (23)
1 3 5 (24)
1 5 3 (24)
3 1 5 (24)
3 5 1 (24)
5 1 3 (24)
5 3 1 (24)
1 3 4 (25)
1 4 3 (25)
3 1 4 (25)
3 4 1 (25)
4 1 3 (25)
4 3 1 (25)
1 2 5 (34)
1 5 2 (34)
2 1 5 (34)
2 5 1 (34)
5 1 2 (34)
5 2 1 (34)
1 2 4 (35)
1 4 2 (35)
2 1 4 (35)
2 4 1 (35)
4 1 2 (35)
4 2 1 (35)
1 2 3 (45)
1 3 2 (45)
2 1 3 (45)
2 3 1 (45)
3 1 2 (45)
3 2 1 (45)
(12) (34) 5
(12) (35) 4
(12) (45) 3
(13) (24) 5
(13) (25) 4
(13) (45) 2
(14) (23) 5
(14) (25) 3
(14) (35) 2
(15) (23) 4
(15) (24) 3
(15) (34) 2
(23) (14) 5
(23) (15) 4
(23) (45) 1
(24) (13) 5
(24) (15) 3
(24) (35) 1
(25) (13) 4
(25) (14) 3
(25) (34) 1
(34) (12) 5
(34) (15) 2
(34) (25) 1
(35) (12) 4
(35) (14) 2
(35) (24) 1
(45) (12) 3
(45) (13) 2
(45) (23) 1
(12) 5 (34)
(12) 4 (35)
(12) 3 (45)
(13) 5 (24)
(13) 4 (25)
(13) 2 (45)
(14) 5 (23)
(14) 3 (25)
(14) 2 (35)
(15) 4 (23)
(15) 3 (24)
(15) 2 (34)
(23) 5 (14)
(23) 4 (15)
(23) 1 (45)
(24) 5 (13)
(24) 3 (15)
(24) 1 (35)
(25) 4 (13)
(25) 3 (14)
(25) 1 (34)
(34) 5 (12)
(34) 2 (15)
(34) 1 (25)
(35) 4 (12)
(35) 2 (14)
(35) 1 (24)
(45) 3 (12)
(45) 2 (13)
(45) 1 (23)
3 (12) (45)
4 (12) (35)
5 (12) (34)
2 (13) (45)
4 (13) (25)
5 (13) (24)
2 (14) (35)
3 (14) (25)
5 (14) (23)
2 (15) (34)
3 (15) (24)
4 (15) (23)
1 (23) (45)
4 (23) (15)
5 (23) (14)
1 (24) (35)
3 (24) (15)
5 (24) (13)
1 (25) (34)
3 (25) (14)
4 (25) (13)
1 (34) (25)
2 (34) (15)
5 (34) (12)
1 (35) (24)
2 (35) (14)
4 (35) (12)
1 (45) (23)
2 (45) (13)
3 (45) (12)
(123) 4 5
(123) 5 4
(124) 3 5
(124) 5 3
(125) 3 4
(125) 4 3
(134) 2 5
(134) 5 2
(135) 2 4
(135) 4 2
(145) 2 3
(145) 3 2
(234) 5 1
(234) 1 5
(235) 1 4
(235) 4 1
(245) 1 3
(245) 3 1
(345) 1 2
(345) 2 1
4 (123) 5
5 (123) 4
3 (124) 5
5 (124) 3
3 (125) 4
4 (125) 3
2 (134) 5
5 (134) 2
2 (135) 4
4 (135) 2
2 (145) 3
3 (145) 2
1 (234) 5
5 (234) 1
1 (235) 4
4 (235) 1
1 (245) 3
3 (245) 1
1 (345) 2
2 (345) 1
4 5 (123)
5 4 (123)
3 5 (124)
5 3 (124)
3 4 (125)
4 3 (125)
2 5 (134)
5 2 (134)
2 4 (135)
4 2 (135)
2 3 (145)
3 2 (145)
1 5 (234)
5 1 (234)
1 4 (235)
4 1 (235)
1 3 (245)
3 1 (245)
1 2 (345)
2 1 (345)
(123) (45)
(124) (35)
(125) (34)
(134) (25)
(135) (24)
(145) (23)
(234) (15)
(235) (14)
(245) (13)
(345) (12)
(45) (123)
(35) (124)
(34) (125)
(25) (134)
(24) (135)
(23) (145)
(15) (234)
(14) (235)
(13) (245)
(12) (345)
(1234) 5
(1235) 4
(1245) 3
(1345) 2
(2345) 1
5 (1234)
4 (1235)
3 (1245)
2 (1345)
1 (2345)
(12345)
```

TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25
□ 1988/$25 □ 1989/$25 □ 1990/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988,1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED: □